La logique équationnelle

Retour sur les signatures et les termes

Soit $\mathcal{X}$ un ensemble de variables. Soit Σ une signature contenant un ensemble dénombrable de symboles de fonction $\{f, g, h, \ldots\}$, chacun ayant une arité.

$\mathcal{T}_{\Sigma,\mathcal{X}}$: l'ensemble de termes sur $\mathcal{X}$ et Σ:

$$\frac{x \in \mathcal{X}}{x \in \mathcal{T}_{\Sigma,\mathcal{X}}} \qquad \frac{t_1, \ldots, t_n \in \mathcal{T}_{\mathcal{X},\Sigma} \quad f/n \in \Sigma}{f(t_1, \ldots, t_n) \in \mathcal{T}_{\Sigma,\mathcal{X}}}$$

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.

$$\frac{}{\Lambda \in \mathbb{N}^*} \qquad \frac{i \in \mathbb{N} \text{ et } p \in \mathbb{N}^*}{ip \in \mathbb{N}^*}$$

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

$$\frac{}{\Lambda \in Pos(t)} \qquad \frac{p \in Pos(t_i) \text{ et } 1 \leq i \leq n}{ip \in Pos(f(t_1, \ldots, t_n))}$$

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 :

$$\frac{}{t|_\Lambda = t} \qquad \frac{t_i|_q = v}{f(t_1, \ldots, t_n)|_{iq} = v}$$

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

- $t[\Lambda/\!/v] = v$
- $f(t_1, \ldots, t_n)[ip/\!/v] = f(t_1, \ldots, t_i[p/\!/v], \ldots, t_n)$

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 $(s[t]_{p.q})[r]_p = s[r]_p$.

Retour sur les interprétations

Exemple : Soit $\Sigma_F = \{z/0, s/1, p/2\}$.

1. $\mathcal{D}$ est l'ensemble $\mathbb{N}$, $\mathcal{I}(z) = 0$, $\mathcal{I}(s)(n) = n+1$ et $\mathcal{I}(p)(n,m) = n+m$.
2. $\mathcal{D}$ est l'ensemble $\mathbb{Z}$, $\mathcal{I}(z) = -5$, $\mathcal{I}(s)(n) = n * 13$ et $\mathcal{I}(p)(n,m) = n * m$.
3. Algèbre syntaxique: $\mathcal{D}$ est l'ensemble de termes sur $\mathcal{X}$ et $\Sigma = \{z, s, p\}$ t.q. $\mathcal{I}(z) = z$, $\mathcal{I}(s)(t) = s(t)$ et $\mathcal{I}(p)(t,u) = p(t,u)$.

Raisonnement équationnel sémantique

Une équation est un couple $s \doteq t$.

Une interprétation $\mathcal{I}$ est un modèle d'un ensemble d'équations $\mathcal{E}$, noté $\mathcal{I} \models \mathcal{E}$, ssi $\mathcal{I}$ est un modèle de chaque équation de $\mathcal{E}$, i.e. $[s]_{\mathcal{I},\sigma} = [t]_{\mathcal{I},\sigma}$ pour toute équation $s \doteq t \in \mathcal{E}$ et valuation σ.

Exemple : La première interprétation sur le transparent "retour sur les interprétations" est un modèle de l'équation $x + y \doteq y + x$.

Conséquence logique équationnelle

L'équation $s \doteq t$ est conséquence logique d'un ensemble d'équations $\mathcal{E}$, noté $\mathcal{E} \models s \doteq t$, ssi chaque modèle de $\mathcal{E}$ est aussi un modèle de $s \doteq t$ ssi $\mathcal{I} \models \mathcal{E}$ implique $\mathcal{I} \models s \doteq t$.

Exemple : Soit la signature $\Sigma_F = \{e/0, i/1, \circ/2\}$ et l'ensemble d'équations $\mathcal{E}$:

$$\begin{array}{lrcl} E1: & (x \circ y) \circ z & \doteq & x \circ (y \circ z) \\ E2: & e \circ x & \doteq & x \\ E3: & i(x) \circ x & \doteq & e \end{array}$$

L'équation $x \circ i(x) \doteq e$ est une conséquence logique de $\mathcal{E}$.

Raisonnement équationnel syntaxique

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

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

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

On note $\mathcal{E} \vdash s \doteq t$ la dérivation de $s \doteq t$ à partir d'un ensemble $\mathcal{E}$.

Exemple

Soit $\mathcal{E} = \{0 + x \doteq x, s(y) + x \doteq s(y + x)\}$.

On derive $s(0) + 3 \doteq 4$ à partir de $\mathcal{E}$ comme suit:

$$\dfrac{\dfrac{\dfrac{s(y) + x \doteq s(y + x) \in \mathcal{E}}{s(y) + x \doteq s(y + x)}\,(subst)}{s(0) + 3 \doteq s(0 + 3)} \qquad \dfrac{\dfrac{\dfrac{0 + x \doteq x \in \mathcal{E}}{0 + x \doteq x}\,(subst)}{0 + 3 \doteq 3}}{s(0 + 3) \doteq s(3)}\,(ctxt)}{s(0) + 3 \doteq s(3)}\,(tran)$$

Théorème de Birkhoff (1933)

Soit $\mathcal{E}$ un ensemble d'équations.

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

Quelques théories intéressantes

L'arithmétique de Presburger

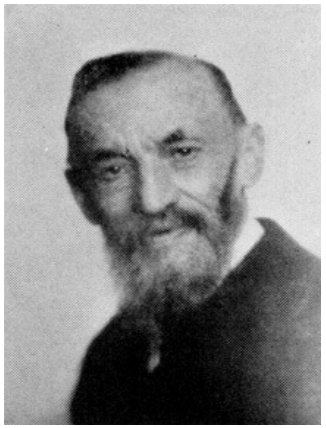
Symboles de fonction: $\{0/0, s/1, +/2\}$
Symboles de prédicat: $\{\doteq /2\}$

$$
\begin{array}{lll}
A1: & \forall x & \neg(s(x) \doteq 0) \\
A2: & \forall x \exists y & \neg(x \doteq 0) \rightarrow x \doteq s(y) \\
A3: & \forall x \forall y & s(x) \doteq s(y) \rightarrow x \doteq y \\
A4: & \forall x & +(x, 0) \doteq x \\
A5: & \forall x \forall y & +(x, s(y)) \doteq s(+(x, y)) \\
SI: & & [P(0) \wedge (\forall x\ P(x) \rightarrow P(s(x)))] \rightarrow \forall x\ P(x)
\end{array}
$$

Résultats

Théorème : La théorie de Presburger est complète et décidable.

L'arithmétique de Peano



Giuseppe Peano (1858 - 1932)

Symboles de fonction: $\{0/0, s/1, +/2, */2\}$
Symboles de prédicat: $\{\doteq /2\}$

$$
\begin{array}{lll}
A1: & \forall x & \neg(s(x) \doteq 0) \\
A2: & \forall x \exists y & \neg(x \doteq 0) \rightarrow x \doteq s(y) \\
A3: & \forall x \forall y & s(x) \doteq s(y) \rightarrow x \doteq y \\
A4: & \forall x & +(x, 0) \doteq x \\
A5: & \forall x \forall y & +(x, s(y)) \doteq s(+(x, y)) \\
A6: & \forall x & *(x, 0) \doteq 0 \\
A6: & \forall x \forall y & *(x, s(y)) \doteq +(*(x, y), x) \\
SI: & & [P(0) \wedge (\forall x\ P(x) \rightarrow P(s(x)))] \rightarrow \forall x\ P(x)
\end{array}
$$

Exercice

Montrer que chaque équation P_i est une conséquence logique de la théorie de Peano :

$P1$	$\forall x$	$+(0, x) \doteq x$
$P2$	$\forall x \forall y$	$s(+(x, y)) \doteq +(s(x), y)$
$P3$	$\forall x$	$+(s(0), x) \doteq s(x)$
$P4$	$\forall x \forall y$	$+(x, y) \doteq +(y, x)$
$P5$	$\forall x \forall y \forall z$	$+(x, +(y, z)) \doteq +(+(x, y), z)$

Résultats pour la théorie de Peano

Une théorie $\mathcal{T}$ est cohérente si la contradiction (formule équivalente à $p \wedge \neg p$) n'est pas prouvable dans $\mathcal{T}$.

Théorème : La théorie de Peano est cohérente.

Théorème : La théorie de Peano n'est pas complète.

Théorème : On ne peut pas prouver la cohérence de la théorie de Peano dans la théorie de Peano elle même.

Ces résultats sont même generalisés ....

Théorèmes d'incomplétude

Kurt Gödel (1906 - 1978)

Les plus célèbres théorèmes de la logique

Soit $\mathcal{T}$ une théorie assez puissant pour formaliser les entiers naturels.

Théorème : Si $\mathcal{T}$ est cohérente ($\mathcal{T}$ ne permet pas de démontrer tous les énonces), alors $\mathcal{T}$ n'est pas complète.

Conséquence: il existe des vérités dans des théories mathématiques qui sont indémontrables. Ce résultat est valable en particulier pour l'arithmétique de Peano qui est donc incomplète. En conséquence, aucun système formel ou axiomatisation ne peut décrire toutes les vérités (propriétés) sur les entiers naturels.

Théorème : Si $\mathcal{T}$ est cohérente, alors la cohérence de $\mathcal{T}$ ne peut pas être prouvée au sein même de la théorie $\mathcal{T}$.

A réfléchir....

- Une chose vraie n'est pas toujours prouvable.
- On ne peut pas donner un jeu d'axiomes définitif pour situer l'ensemble de toutes les mathématiques sur une base axiomatique.
- On ne peut pas axiomatiser toutes les mathématiques.