Préliminaires

Expressions, induction, évaluation, *etc.*

Lionel Vaux Auclair

I2M, université d'Aix-Marseille

M2 IMD

Syntaxe et sémantique

Deux gros mots chargés d'histoire :

- syntaxe : des expressions (les termes, les formules, les programmes)
- sémantique : leurs valeurs (les éléments d'une structure, les valeurs de vérité, les fonctions calculées)

Un polynôme c'est une expression avec des $+$ et des $\times$

On fixe un ensemble $\mathcal{V}$ de variables (ou indéterminées).

Une expression polynomiale est une expression construite à partir des variables et des constantes 0 (le polynôme nul) et 1 (le polynôme constant unitaire), par application des constructeurs binaires $+$ et $\times$, et du constructeur unaire $-$.

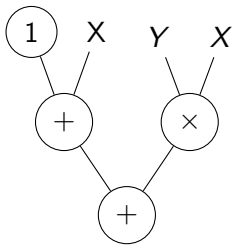
Exemple

$$0 \qquad -(-X) \qquad X+(Y+Z) \qquad (X\times Y)+(X+1)$$

À ce stade, $X \neq -(-X)$ et $X+(Y+Z) \neq (X+Y)+Z$, vu que ça ne s'*écrit* pas pareil.

Un polynôme c'est un arbre avec des $+$ et des $\times$

$(X \times Y) + (X + 1) =$



Expressions

Une expression = un mot construit par l'application itérée de symboles d'arité fixée.

Définition

Une signature = un ensemble $\mathcal{S}$ de symboles, chacun muni d'une arité (donnée par une fonction $a : \mathcal{S} \to \mathbf{N}$).

Définition

Étant donné un ensemble $\mathcal{A}$ d'atomes, l'ensemble des expressions sur $\mathcal{S}$ est le plus petit ensemble de mots sur l'alphabet $\mathcal{A} \cup \mathcal{S} \cup \{ \langle , \rangle , ; \}$ contenant $\mathcal{A}$ et clos par les fonctions : $(w_1, \ldots, w_{a(s)}) \mapsto s\langle w_1; \ldots; w_{a(s)} \rangle$ pour $s \in \mathcal{S}$.

Expressions polynomiales

Une expression polynomiale est une expression sur la signature $\{+, \times, -, 0, 1\}$ avec $a(+) = a(\times) = 2$, $a(-) = 1$, $a(0) = 0$ et $a(1) = 0$, avec les variables comme atomes :

- une variable X est une expression atomique ;
- si P et Q sont des expressions données, $+\langle P; Q\rangle$ est une nouvelle expression (qu'on note le plus souvent $P + Q$) ;
- le symbole 1 est une constante (= d'arité 0) donc $1\langle\rangle$ est toujours une expression (qu'on note le plus souvent 1).

Une expression = un arbre

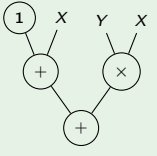
La correspondance entre arbres et expressions est univoque et transparente : une expression a une taille et une hauteur, un ensemble de feuilles (ses atomes), *etc.*

$$\#x = 1 \qquad \#s\langle w_1; \ldots; w_n\rangle = 1 + \sum_{i=1}^{n} \#w_i$$

$$h(x) = 1 \qquad h(s\langle w_1; \ldots; w_n\rangle) = 1 + \max_{i=1}^{n} h(w_i)$$

$$\mathcal{A}(x) = \{x\} \qquad \mathcal{A}(x)(s\langle w_1; \ldots; w_n\rangle) = \bigcup_{i=1}^{n} \mathcal{A}(w_i)$$

Exemple

Avec $P = (X \times Y) + (X + 1) =$ 

$: \begin{cases} \#P = 7 \\ h(P) = 3 \\ \mathcal{A}(P) = \{X, Y\} \end{cases}$.

Raisonnement par induction

On peut raisonner (ou définir des choses) par induction sur les arbres et les expressions :

- pour démontrer un résultat sur tous les arbres, il suffit de le démontrer sur un arbre quelconque, en supposant le résultat valide sur tous ses sous arbres stricts ;
- pour définir une fonction sur les arbres il suffit de définir l'image d'un arbre quelconque, en supposant la fonction définie sur tous ses sous arbres stricts ;

parce que la relation « sous arbre » est *bien fondée*.

Structures définies inductivement

Une expression polynomiale c'est une variable, ou une somme d'expressions polynomiales, ou un produit d'expressions polynomiales, ou l'opposé d'une expression polynomiale, ou 0 ou 1 (et rien d'autre) :

$$\mathcal{E}_{pol}(\mathcal{V}) \ni P, Q, R, \ldots ::= X \mid P + Q \mid P \times Q \mid -P \mid 0 \mid 1$$

où $X \in \mathcal{V}$

Une expression sur la signature $\mathcal{S}$ et les atomes $\mathcal{A}$, c'est un atome ou l'application d'un symbole de $\mathcal{S}$ à des sous expressions, en respectant l'arité (et rien d'autre) :

$$\mathcal{E}(\mathcal{A}, \mathcal{S}) \ni u, v, w, \ldots ::= x \mid s\langle w_1; \ldots; w_{a(s)}\rangle$$

où $x \in \mathcal{A}$, $s \in \mathcal{S}$

Valeur d'une expression polynomiale

On peut définir la valeur d'un polynôme, *en fonction* de la valeur de ses variables, prise dans un anneau A quelconque. On généralisera ça avec le calcul des prédicats.

Soit $v : \mathcal{V} \to \mathrm{A}$ (une valeur pour chaque variable), on étend v à tous les polynômes en posant (inductivement)

$$\begin{aligned} v(1) &= 1_{\mathrm{A}} \\ v(0) &= 0_{\mathrm{A}} \\ v(-P) &= -_{\mathrm{A}} v(P) \\ v(P+Q) &= v(P) +_{\mathrm{A}} v(Q) \\ v(P \times Q) &= v(P) \times_{\mathrm{A}} v(Q) \end{aligned}$$

En général, $\mathcal{V}$ est fini, par exemple $\mathcal{V} = \{X, Y\}$ et on note $v = (a, b)$ si $v(X) = a$ et $v(Y) = b$, et alors on écrit plutôt $P(a, b)$ au lieu de $v(P)$.

Fonctions polynomiales

Une fonction polynomiale, c'est une fonction de la forme

$$\begin{aligned} \hat{P} : \mathrm{A}^{\mathcal{V}} &\to \mathrm{A} \\ v &\mapsto v(P) \end{aligned}$$

avec P un polynôme fixé.

- Ça dépend de l'ensemble de coefficients A qu'on considère.
- En général, on peut avoir $\hat{P} = \hat{Q}$ avec $P \neq Q$ (par exemple si $\mathrm{A} = \mathrm{Z}/2\mathrm{Z}$, $\hat{0} = \widehat{X + X}$).

On dit que P et Q sont équivalentes et on note $P \equiv Q$ si $\hat{P} = \hat{Q}$ dans tout anneau A.

Un avant-goût du théorème de complétude

- Ce qu'on appelle polynôme (à coefficients entiers) d'habitude, ce sont plutôt les expressions polynomiales modulo les identités usuelles : $P + Q = Q + P$, $1 \times P = P$, *etc.*

  (= les axiomes de la structure d'anneau)

- On note $\sim$ la plus petite relation d'équivalence contenant ces identités et compatible avec les constructeurs (par exemple $P \sim P' \Rightarrow P + Q \sim P' + Q$).

Lemme (Correction)

Si $P \sim Q$ alors $P \equiv Q$.

Démonstration: $\equiv$ est une relation d'équivalence qui contient les axiomes des anneaux et qui est compatible avec les opérations. □

Un avant-goût du théorème de complétude

- Ce qu'on appelle polynôme (à coefficients entiers) d'habitude, ce sont plutôt les expressions polynomiales modulo les identités usuelles : $P + Q = Q + P$, $1 \times P = P$, *etc.*

  (= les axiomes de la structure d'anneau)

- On note $\sim$ la plus petite relation d'équivalence contenant ces identités et compatible avec les constructeurs (par exemple $P \sim P' \Rightarrow P + Q \sim P' + Q$).

Lemme (Correction)

Si $P \sim Q$ alors $P \equiv Q$.

Lemme (Complétude)

On a $P \sim Q$ ssi $P \equiv Q$.

Démonstration: Les polynômes (les expressions polynomiales modulo $\sim$) forment un anneau.

□

Fonctions polynomiales dans l'anneau des polynômes

- Si P est une expression polynomiale, on note $\overline{P}$ le polynôme associé (la classe de P modulo $\sim$).
- On a : $\overline{P+Q} = \overline{P} + \overline{Q}$, $\overline{P \times Q} = \overline{P}\,\overline{Q}$, $\overline{-P} = -\overline{P}$, $\overline{1} = 1$, $\overline{0} = 0$.
- L'évaluation c'est la substitution : si $\mathcal{A}(P) = \{X_1, \ldots, X_n\}$ et $v(X_i) = \bar{Q}_i$,

$$\hat{P}(v) = v(P) = \overline{P[X_1 := Q_1, \ldots, X_n := Q_n]}\ .$$

Exemple

Si $P = X \times X$ et $v(X) = \overline{Y+Z}$ alors $v(P) = \overline{(Y+Z)\times(Y+Z)} = \overline{Y}^2 + 2\overline{Y}\,\overline{Z} + \overline{Z}^2$.

Un avant-goût du théorème de complétude

- Ce qu'on appelle polynôme (à coefficients entiers) d'habitude, ce sont plutôt les expressions polynomiales modulo les identités usuelles : $P + Q = Q + P$, $1 \times P = P$, *etc.*

  (= les axiomes de la structure d'anneau)

- On note $\sim$ la plus petite relation d'équivalence contenant ces identités et compatible avec les constructeurs (par exemple $P \sim P' \Rightarrow P + Q \sim P' + Q$).

Lemme (Correction)

Si $P \sim Q$ alors $P \equiv Q$.

Lemme (Complétude)

On a $P \sim Q$ ssi $P \equiv Q$.

Démonstration: Les polynômes (les expressions polynomiales modulo $\sim$) forment un anneau.
En choisissant $v(X) = \overline{X}$, on obtient $v(P) = \overline{P}$.
Si $P \equiv Q$, alors $v(P) = v(Q)$, donc $\overline{P} = \overline{Q}$ et donc $P \sim Q$. □