

Préliminaires

Expressions, induction, évaluation, *etc.*

Lionel Vaux Auclair

I2M, université d'Aix-Marseille

Logique et calculabilité

M1 Mathématiques et applications, 2020–2021

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**).

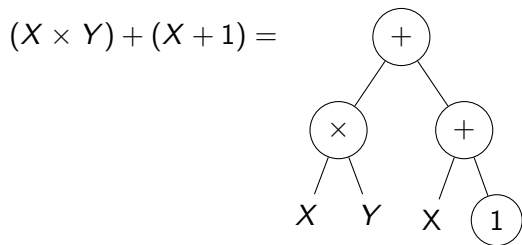
Une **expression polynomiale** est une expression construite à partir des variables et des constantes **0** (le polynôme nul) et **1** (le polynôme constant unitaire), par application des constructeurs binaires $+$ et $\times$, et du constructeur unaire $-$.

Exemple

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

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 $\times$



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 $a : \mathcal{S} \rightarrow \mathbb{N}$).

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 : $(w_1, \dots, w_{a(s)}) \mapsto s \langle w_1; \dots; w_{a(s)} \rangle$ 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.

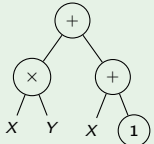
$$\#x = 1 \qquad \#s\langle w_1; \dots; w_n \rangle = 1 + \sum_{i=1}^n \#w_i$$

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

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

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) :

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

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) :

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

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

$$v(1) = 1_A$$

$$v(0) = 0_A$$

$$v(-P) = -_A v(P)$$

$$v(P + Q) = v(P) +_A v(Q)$$

$$v(P \times Q) = v(P) \times_A v(Q)$$

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

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

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 $A = \mathbb{Z}/2\mathbb{Z}$, $\hat{0} = \widehat{X + X}$).

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 $\mathcal{A}(P) = \{X_1, \dots, X_n\}$ et $v(X_i) = \bar{Q}_i$,

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

Exemple

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

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 $P \sim Q$. □

Calcul propositionnel

On fixe un ensemble infini dénombrable $\mathcal{V}_p$ de **variables propositionnelles**, notées $X, Y, \dots$

Définition

L'ensemble $\mathcal{F}_p$ des **formules propositionnelles** est l'ensemble des expressions de la forme :

$$A, B, \dots ::= X \mid A \wedge B \mid A \vee B \mid \neg A \mid A \Rightarrow B \mid A \Leftrightarrow B \mid \top \mid \perp$$

= les expressions sur la signature $\{\wedge, \vee, \neg, \Rightarrow, \Leftrightarrow, \top, \perp\}$.

Les tables de la véritable vérité vraie (100% garanti)

La validité d'une formule propositionnelle se *calcule* dans $\mathbf{B} = \{0, 1\}$:

A	B	$A \wedge B$	$A \vee B$	$\neg A$	$A \Rightarrow B$	$A \Leftrightarrow B$	$\top$	$\perp$
0	0	0	0	1	1	1	1	0
0	1	0	1	1	1	0	1	0
1	0	0	1	0	0	0	1	0
1	1	1	1	0	1	1	1	0

- On voit les connecteurs comme des opérations.
- La valeur d'une expression se déduit *inductivement* de celle de ses sous-expressions.

Les tables de la véritable vérité vraie (100% garanti)

La validité d'une formule propositionnelle se *calcule* dans $\mathbf{B} = \{0, 1\}$:

A	B	$A \wedge B$	$A \vee B$	$\neg A$	$A \Rightarrow B$	$A \Leftrightarrow B$	$\top$	$\perp$	X
0	0	0	0	1	1	1	1	0	?
0	1	0	1	1	1	0	1	0	?
1	0	0	1	0	0	0	1	0	?
1	1	1	1	0	1	1	1	0	?

- ▶ On voit les connecteurs comme des opérations.
- ▶ La valeur d'une expression se déduit *inductivement* de celle de ses sous-expressions.

Les tables de la véritable vérité vraie (100% garanti)

La validité d'une formule propositionnelle se *calcule* dans $\mathbf{B} = \{0, 1\}$:

A	B	$A \wedge B$	$A \vee B$	$\neg A$	$A \Rightarrow B$	$A \Leftrightarrow B$	$\top$	$\perp$	X
0	0	0	0	1	1	1	1	0	?
0	1	0	1	1	1	0	1	0	?
1	0	0	1	0	0	0	1	0	?
1	1	1	1	0	1	1	1	0	?

- ▶ On voit les connecteurs comme des opérations.
- ▶ La valeur d'une expression se déduit *inductivement* de celle de ses sous-expressions.
- ↪ Une **distribution de valeurs de vérités** $d : \mathcal{V}_p \rightarrow \mathbf{B}$ s'étend en une **valuation** de toutes les formules $A \in \mathcal{F}_p \mapsto d(A) \in \mathbf{B}$.
- ▶ A est une **tautologie** ssi $d(A) = 1$ pour toute dvv d .

Quelques tautologies

$$A \Rightarrow A \quad (A \wedge B) \Rightarrow A \quad A \Rightarrow (A \vee B)$$

$$((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$$

$$A \vee (A \Rightarrow B) \quad (\neg A) \vee A$$

...

Quelques tautologies

$$A \Rightarrow A \quad (A \wedge B) \Rightarrow A \quad A \Rightarrow (A \vee B)$$

$$((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$$

$$A \vee (A \Rightarrow B) \quad (\neg A) \vee A$$

...

↗ Vérifiez

Priorités et associations

On donne les priorités

$$\{\neg\} > \{\wedge, \vee\} > \{\Rightarrow\} > \{\Leftrightarrow\}$$

donc on écrit par exemple

$$\neg A \vee B \Leftrightarrow A \Rightarrow B = ((\neg A) \vee B) \Leftrightarrow (A \Rightarrow B).$$

On note

$$A \wedge B \wedge C = (A \wedge B) \wedge C$$

$$A \vee B \vee C = (A \vee B) \vee C$$

$$A \Rightarrow B \Rightarrow C = A \Rightarrow (B \Rightarrow C)$$

donc on écrit par exemple

$$A \wedge B \wedge C \Rightarrow A \wedge B \Rightarrow B \wedge C = (A \wedge B) \wedge C \Rightarrow (A \wedge B \Rightarrow B \wedge C)$$

Quelques tautologies

$$A \Rightarrow A \quad A \wedge B \Rightarrow A \quad A \Rightarrow A \vee B$$

$$(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow A \Rightarrow C$$

$$A \vee (A \Rightarrow B) \quad \neg A \vee A$$

...

Équivalence

On dit que A et B sont **équivalentes** ssi, pour toute dvv d , $d(A) = d(B)$: on note $A \equiv B$.

Lemme

On a $A \equiv B$ ssi $A \Leftrightarrow B$ est une tautologie .

Démonstration: On a $d(A \Leftrightarrow B) = 1$ ssi $d(A) = d(B)$.



Équivalences classiques

Le quotient $\mathcal{F}_p/\equiv$ est un treillis ...

$$\begin{aligned} A \wedge B &\equiv B \wedge A & (A \wedge B) \wedge C &\equiv A \wedge (B \wedge C) & A \wedge (A \vee B) &\equiv A \\ A \vee B &\equiv B \vee A & (A \vee B) \vee C &\equiv A \vee (B \vee C) & A \vee (A \wedge B) &\equiv A \\ & & \text{(et donc : } A \wedge A &\equiv A & A \vee A &\equiv A) \end{aligned}$$

... distributif ...

$$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C) \quad A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$$

... borné et complémenté...

$$\begin{aligned} A \wedge \top &\equiv A & A \vee \perp &\equiv A & A \wedge \neg A &\equiv \perp & A \vee \neg A &\equiv \top \\ & & \text{(et donc : } A \wedge \perp &\equiv \perp & A \vee \top &\equiv \top) \end{aligned}$$

$\rightsquigarrow$ c'est une algèbre de Boole.

Équivalences classiques

Le quotient $\mathcal{F}_p/\equiv$ est un treillis ...

$$\begin{aligned} A \wedge B &\equiv B \wedge A & (A \wedge B) \wedge C &\equiv A \wedge (B \wedge C) & A \wedge (A \vee B) &\equiv A \\ A \vee B &\equiv B \vee A & (A \vee B) \vee C &\equiv A \vee (B \vee C) & A \vee (A \wedge B) &\equiv A \\ & & \text{(et donc : } & A \wedge A &\equiv A & A \vee A &\equiv A) \end{aligned}$$

... distributif ...

$$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C) \quad A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$$

... borné et complémenté...

$$\begin{aligned} A \wedge \top &\equiv A & A \vee \perp &\equiv A & A \wedge \neg A &\equiv \perp & A \vee \neg A &\equiv \top \\ & & \text{(et donc : } & A \wedge \perp &\equiv \perp & A \vee \top &\equiv \top) \end{aligned}$$

$\rightsquigarrow$ c'est une algèbre de Boole.

$\rightsquigarrow$ Vérifiez

Équivalences classiques

Lois de De Morgan :

$$\neg\neg A \equiv A \quad \neg(A \wedge B) \equiv \neg A \vee \neg B$$

$$\neg\top \equiv \perp$$

$$\neg(A \vee B) \equiv \neg A \wedge \neg B$$

$$\neg\perp \equiv \top$$

Autour de l'implication :

$$A \Rightarrow B \equiv \neg A \vee B \equiv \neg B \Rightarrow \neg A$$

$$(A \wedge B) \Rightarrow C \equiv A \Rightarrow B \Rightarrow C$$

$$\neg(A \Rightarrow B) \equiv A \wedge \neg B$$

$$\neg A \equiv A \Rightarrow \perp$$

Équivalences classiques

Lois de De Morgan :

$$\neg\neg A \equiv A \quad \neg(A \wedge B) \equiv \neg A \vee \neg B$$

$$\neg\top \equiv \perp$$

$$\neg(A \vee B) \equiv \neg A \wedge \neg B$$

$$\neg\perp \equiv \top$$

Autour de l'implication :

$$A \Rightarrow B \equiv \neg A \vee B \equiv \neg B \Rightarrow \neg A$$

$$(A \wedge B) \Rightarrow C \equiv A \Rightarrow B \Rightarrow C$$

$$\neg(A \Rightarrow B) \equiv A \wedge \neg B$$

$$\neg A \equiv A \Rightarrow \perp$$

↪ Vérifiez

L'équivalence est une congruence

Autrement dit, elle est compatible avec les constructeurs de formules :

Lemme

Si $A \equiv A'$ et $B \equiv B'$ alors

$$\neg A \equiv \neg A', \quad A \wedge B \equiv A' \wedge B', \quad A \Rightarrow B \equiv A' \Rightarrow B', \dots$$

Démonstration: Par exemple $A \wedge B \equiv A' \wedge B'$ car, pour toute dvv d ,
 $d(A \wedge B) = \min(d(A), d(B)) = \min(d(A'), d(B')) = d(A' \wedge B')$.



L'équivalence est une congruence

Autrement dit, elle est compatible avec les constructeurs de formules :

Lemme

Si $A \equiv A'$ et $B \equiv B'$ alors

$$\neg A \equiv \neg A', \quad A \wedge B \equiv A' \wedge B', \quad A \Rightarrow B \equiv A' \Rightarrow B', \dots$$

Démonstration: Par exemple $A \wedge B \equiv A' \wedge B'$ car, pour toute dvv d ,
 $d(A \wedge B) = \min(d(A), d(B)) = \min(d(A'), d(B')) = d(A' \wedge B')$. □

On peut donc établir la validité des formules *par le calcul* :

$$\begin{aligned} (A \Rightarrow B) \vee (B \Rightarrow C) &\equiv (\neg A \vee B) \vee (\neg B \vee C) \\ &\equiv \neg A \vee (B \vee \neg B) \vee C \\ &\equiv \neg A \vee \top \vee C \\ &\equiv \top \end{aligned}$$

Jeux de connecteurs complets

Théorème

Toute formule propositionnelle est équivalente à une formule n'utilisant que les connecteurs $\wedge$ et $\neg$ (ou $\vee$ et $\neg$, ou encore $\Rightarrow$ et $\neg$, ou ...).

Démonstration: Faisons le avec $\wedge$ et $\neg$. On a :

$$A \vee B \equiv \neg(\neg A \wedge \neg B)$$

$$A \Rightarrow B \equiv \neg A \vee B \equiv \neg(A \wedge \neg B)$$

$$A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A) \equiv \neg(A \wedge \neg B) \wedge \neg(B \wedge \neg A)$$

$$\perp \equiv X \wedge \neg X$$

$$\top \equiv \neg(X \wedge \neg X)$$

et on peut donc remplacer inductivement tous les connecteurs autres que $\wedge$ et $\neg$. □

Donc, à équivalence près, on peut raisonner inductivement sur $\mathcal{F}_{\wedge, \neg} ::= X \mid A \wedge B \mid \neg A$.