

①

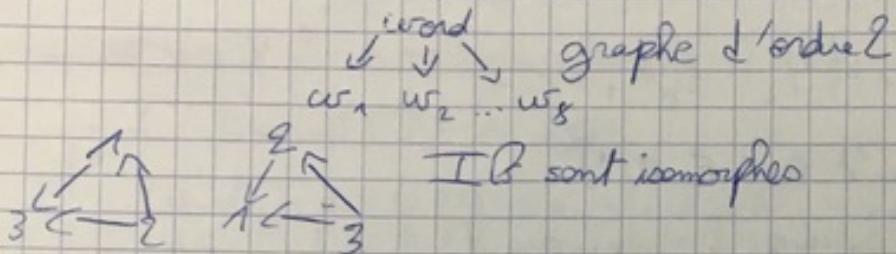
Logique du Première ordre

Bly sun Mastercorp

mathématiques: la science dont l'objet d'étude est les entités abstraites.

- ## • Le problème de la définition

Définition classique: Dans un dictionnaire mot : = [phrase] soit $w_1 w_2 \dots w_n$



Point Définition par induction: On souhaite définir un type d'objet noté \mathcal{E} . Le faire par induction c'est :

par induction, c'est:

- se donner à, $a_2 \dots a_n$ arbitraires des objets qui seront de type \mathcal{G}
 - se donner des constructeurs/opérateurs $\square_1, \square_2 \dots \square_{k_2}$, et leurs respectives r_1, r_2, \dots, r_{k_2}
 - un nombre d'objet qu'on associe ensemble

mumi de regis:

si t_1, \dots, t_r sont de type \mathcal{C} alors $\square_i t_1 \dots t_r$ est de type \mathcal{C}
 • condition d'arrêt : nombre d'étapes

Indication : on écrira "condition d'arrêt w" pour signifier [ça s'arrête] (peu le nombre d'étapes finies) $\text{L'étape intitulée "t" est la } n\text{-ième étape}$

Example: $\#B$ Atomes
G Opérations
G Conditionnement

Le type int est équivalent à entier naturel

Exercise 2

G Gabrusomus

68

and

Complexos

Decrier Bo Gabuzomeu

Étape 0 :

Step 1:

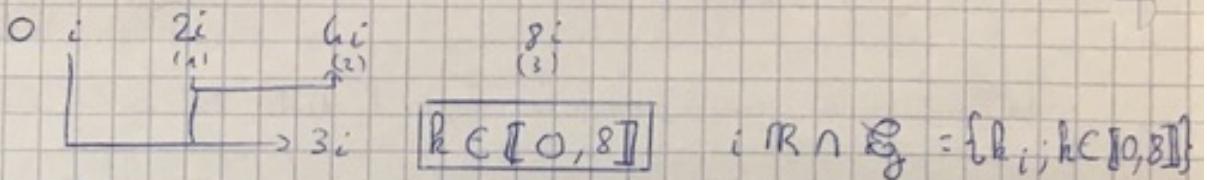
1; i, 42

	+	1	i	42
1		2	42	43
i		1+i	2i	42i
42		43	42+i	84

$$\begin{array}{c|ccccc} * & 1 & i & 42 & 0 & 1-i \\ \hline 1 & 1 & 1+i & 1 & 2 & 2i \\ i & 0 & i & 0 & 42+i & 84 \\ 42 & 42 & 4+i & 42 & & \end{array}$$

② Étape 2: + 0 1 i 2 i 42 2 1+i 43 42+i 84

Bon quelques valeurs de R . A-t-on $R \subseteq$: Gabuzoneu



Exercice: Smurf

AB: "Pluie" et "Blanc"

O: $\{\text{smurf}\} \in \{\text{; ; }\}$; ta. { sont des smurfs
 α -smurf}

$$\left\{ \begin{array}{l} = \{ \dots \} \\ \alpha = \alpha_1 \dots \alpha_n \end{array} \right\} \vdash \alpha_2 \dots \{ \alpha_1 \dots \alpha_{n-1}$$

C: condition d'avant R ($\in \mathbb{N}^*$)

Peut-on construire R telle que assez grand?

C'est impossible par récurrence!

Pour tout $k \geq 1$: tout smurf connaît mon atomique à au moins 5 caractères

(I) atomes ≥ 4 lettres

↳ Cas 1: atome $\geq 1 + 4$ lettres

↳ Cas 2: atome atome $\geq 4 - 1 + 4 - 1 \geq 5$ lettres

(II) Si w et z sont des smurfs non atomiques avec au moins 5 caractères

$$\left[\begin{array}{l} w \\ \pi(w) \\ z \\ \pi(z) \end{array} \right] \geq 1 + 5 \geq 5 \text{ caractères}$$

$$\text{Cas 2 } w = w_1 \dots w_n \quad z = z_1 \dots z_m \quad n \geq 5 \quad m \geq 5 \quad \geq 5 - 1 + 5 - 1 \geq 5$$

(III) Tout smurf non atomique a au moins 5 caractères ou est à au moins 6 caractères et n'est pas atomique donc n'est pas un smurf

II / Formules Propositionnelles

On se donne:

• Δ : alphabet latin majuscules avec indices éventuels

(variables prop) A; B; ...; Z; λ_{a_2} ; H; A_1 ; ...

• Connexions de la Logique classique $\wedge \vee \Rightarrow (\Rightarrow)$ $\top \perp$

AB: élément de Δ mais aussi \top et \perp

O: Si φ et ψ sont des formules logiques d'ordre O, alors $\wedge \varphi \psi \Rightarrow \varphi \psi \top \varphi$

C: condition w

$\vee \varphi \psi \Leftrightarrow \varphi \psi$

Exemples:

Logique du premier ordre

- $A \wedge A T \in F_0$ ($A \wedge T$) jet
- $\wedge V A B C \in F_0$ ($A \vee B$) ^{don} $\wedge C$
- $\Rightarrow (\Rightarrow) \wedge V \neg E P I T A$ $((((\neg E) \vee P) \wedge I) (\Rightarrow T) \Rightarrow A)$
- $\wedge (\wedge \wedge A A A) A$ $\{$ on n'est pas un élément de F_0
 $\} \quad \underbrace{\quad \quad \quad \quad}_{\text{?}}$

Définition: Soit Σ un alphabet c'est à dire un ensemble de objets appelés caractères ou symboles.

De façon induire :

- atomes: tout élément $w \in \Sigma$ est un mot. De plus, on désigne par ϵ un mot vide.
- constructions: si w est un mot sur Σ et x un mot sur Σ . Alors wx (la concaténation) est un mot sur Σ .
- condition d'arrêt: w

(orthographe?)

Vocabulaire: l'ensemble des mots sur Σ , noté Σ^* , s'appelle stan de Kleene

Exemple: $\{0; 1\}^*$ mots binaires

$\{0; 1; 2\}^* \setminus \{\epsilon\}$ désigne l'ensemble des représentants décimaux de N.G.P'

l'ensemble des variables l'ensemble des appelle système décimal.
 propriétés logique

$(\sigma \cup \mathcal{C})^* \not\models F_0$ $\models = \models$ sans égalité

Exemple: 777 AAA $\in (\sigma \cup \mathcal{C})^*$ mais 777AAA $\notin F_0$.

$\varphi \in F_0 \Leftrightarrow A \in F_0 \rightarrow \neg A \in F_0 \rightarrow \neg(\neg A) \in F_0 \rightarrow 777A \in F_0$
 $\varphi \in F_0$

Procédure de vérification d'une formule de F_0 :

Entrée: $\varphi \in (\sigma \cup \mathcal{C})$

Objectif: tester si $\varphi \in F_0$

Procédure: On écrit $\varphi = S_1 S_2 \dots S_n$ où $S_i \in \sigma \cup \mathcal{C}$ ($\{T, L\} \rightarrow \mathbb{Z}$)

- On définit v : ($\begin{matrix} \text{V} & \rightarrow & \mathbb{Z} \\ \text{T} & \rightarrow & -1 \end{matrix}$)

$(\begin{matrix} \text{V} & \rightarrow & \{0, 1\} \\ \text{T} & \rightarrow & 1 \end{matrix}) \rightarrow \mathbb{Z}$

$T \rightarrow 0$

On détermine successivement les valeurs $\sum_{i=1}^k v(s_i)$ pour $k \leq N$

Condition d'arrêt: on rencontre $R \in \mathbb{N}$ tel que $\sum_{s=1}^R \alpha(s) = -1$

on on a calculé toutes les valeurs de T_{an} (par 2)

Théorème : L'algorithme PCF₀ s'arrête en remplaçant les deux conditions simultanément

Exemplos: $\begin{array}{ccccccccc} & \wedge & \wedge & \wedge & A & A & \bar{Z} \\ 0 & 1 & 1 & 1 & -1 & -1 & -1 \\ \Sigma_0 & 1 & 2 & 3 & 2 & 1 & 0 \rightarrow \text{stop } k=7 \end{array}$ Gm me trouxe para -1 donc $AAA\bar{A}\bar{Z}eff$.

Remarque: Ce théorème est vraisemblablement à publier

Exemple 2: $\begin{array}{ccc} 7 & A & A \\ 0 & -1 & -1 \\ \Sigma & 0 & -1 \end{array}$ $7AA \notin F$. $\Rightarrow 77C = 11VEAITA$ Les conditions sont remplie par C.

Démonstration : par induction sur la construction des formules, on prouve le sens direct :

Atomes : $\varphi \in \mathcal{G} \cup \{\top, \perp\}$ avec $\varphi = S_i$ ou $\varphi(S_j) = -1$ le cas est établi par récurrence.

Construction: Domine ne^r pe^t Psi abo^m f₅ Gm. Agape!

criterio octavo

$$\begin{array}{c|cccc} \text{Gra de } Q & n_1 & n_2 & \dots & n_n \\ \hline \sigma & \sigma(n_1) & \sigma(n_2) & \dots & \sigma(n_n) \\ \hline \sum \sigma & \sigma(n_{i+1}) & \sigma(n_i) & \dots & \sigma(n_1) = 1 \\ i & 13 & 2 & \dots & 1 \end{array}$$

$$\sum B_i \sigma(B_i)$$

On va écrire pour amplifier

{ Étape 1 à valeur a
 Étape k à valeur $\rightarrow b$ ($k \in [1, n-1]$)
 Étape n à valeur b

Etudios 1 44:

$$\begin{aligned} & \psi \psi \psi s_1 \dots s_n b_1 \dots b_m \\ & v \vdash v(s_1) v(s_n) v(b_1) \dots v(b_m) \\ & \sum_k v(s_1) + v(s_n) \xrightarrow{\quad} v(s_1) + v(s_n) \\ & -1+1 \xrightarrow{\quad} 0 \\ & \sim 0 \\ & -1 = \sum_k v(s_k) \end{aligned}$$

$$\text{Grade 7Q} \quad \sum_{k=1}^n a_k = a_1 + a_2 + \dots + a_n$$

$\psi \wedge B_1 \dots B_m$	\vdash
$\vdash \psi$	\vdash

Le critère est rempli pour 100

$$\text{Anisi} \Leftrightarrow \neg(\top) = \neg(\vee) = \neg(\Rightarrow) = \neg(\equiv) = 1$$

La raison et les conclusions bibliques

Récapitque: Supposons: $\varphi \in (\nu \cup \mathcal{C})^* \setminus F$.

1^{er} cas : • φ contient un connecteur logique de \mathcal{C} qui a au moins un argument réciproque.

2nd cas : • φ contient un sous mot $\omega = \sigma_i \dots \sigma_n \in F_0$ algébre $\varphi = \sigma_1 \dots \sigma_n$ [logique de preuve ③] (trop d'argent)

Dans le 1st cas, la procédure n'arrive pas à -1
Dans le 2nd cas, la procédure tombe à -1 si $k < n$

exo : formaliser cette correspondance

Sémantique de F_0 (point de vue de Tarski)

Par induction :

Atomes : $\|T\| = \text{Vrai}$

$\|\perp\| = \text{Faux}$

Notation si $\varphi \in F_0$ sa sémantique sera notée $\|\varphi\|$

Pour tout $toto \in V$, on aura : une fonction $\nabla : \omega \rightarrow \{\text{vrai}, \text{faux}\}$ étant donné au moins $\|toto\| = \nabla(toto)$

Vocabulaire : ∇ est appelé assignation de valeurs aux variables

Ainsi $\nabla \models \varphi \wedge \psi : \omega \rightarrow \{\text{vrai}, \text{faux}\}$ on a $\|\perp\|_\nabla = \text{faux}$ et $\|T\|_\nabla = \text{vrai}$

Construction : Soient $\varphi \in F_0$ et $\psi \in F_0$

[Tarski] $\|\wedge \varphi \psi\| = \text{vrai} \Leftrightarrow \|\varphi\| = \text{vrai}$ et $\|\psi\| = \text{vrai}$

etc ... $\|\vee \varphi \psi\|_\nabla = \text{vrai} \Leftrightarrow \|\varphi\|_\nabla = \text{vrai}$ ou $\|\psi\|_\nabla = \text{vrai}$

Remarque : on définit alors $\|\cdot\|_\nabla$ au moyen d'une proposition algébrique de morphisme

plat : $s(*ab) = *s(a)s(b)$

normal : $s(a * b) = s(a) * s(b)$

Définition : On dit que $\varphi \in F_0$ et $\psi \in F_0$ sont sémantiquement équivalents lorsque :

$\forall \nabla : \omega \rightarrow \{\text{vrai}, \text{faux}\} \quad \|\varphi\|_\nabla = \|\psi\|_\nabla$

Notation : On pourra écrire $\varphi \equiv \psi \Rightarrow$ en pratique table de vérité

Cours 2 :

Rappel : φ et ψ sont sémantiquement équivalents lorsque pour tout $\lambda : \omega \rightarrow \{\text{vrai}, \text{faux}\}$

$$\|\varphi\|_\lambda = \|\psi\|_\lambda \text{ On note alors } \varphi \equiv \psi$$

Exemple : Loi de Morgan $\neg(A \wedge B) \equiv \neg A \vee \neg B$

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

$$\neg\neg A \equiv A$$

Logique classique Involution de \neg

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

$$A \vee A = A \wedge A \quad A \wedge A \neq A \quad A \wedge A = A$$

L'égalité est syntaxique \equiv \equiv \equiv signifie une égalité sémantiquement

Cas de la loi de Peirce : $P \Rightarrow Q \Rightarrow P$

$$(P \Rightarrow Q) \Rightarrow P$$

$$P \Rightarrow (Q \Rightarrow P)$$

P	Q	$P \Rightarrow Q$	$(P \Rightarrow Q) \Rightarrow P$	$Q \Rightarrow P$	$P \Rightarrow (Q \Rightarrow P)$
0	0	1	0	1	1
0	1	1	0	0	1
1	0	0	1	1	1
1	1	1	1	1	1

④

Loi de Peirce: $P \Rightarrow (Q \Rightarrow P)$ est une tautologie

Vocabulaire: Ψ est une tautologie lorsque $\Psi \models T$

Consequence: $\Delta P \Rightarrow Q \Rightarrow \Delta$ est en fait AMBIGU !! \Rightarrow non associativité.

\Rightarrow
 \Rightarrow

donc
d'où

Implications connecteurs logiques

l'édition \rightarrow (calcul des récurrences)

On verra la différence entre l'édition et l'implication.

Propriétés: $A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$ }
 $A \vee (B \vee C) \equiv (A \vee B) \vee C$ } Associativité

Propriété: $\Psi \equiv \Psi$ si et seulement si, $\Psi \models \Psi$ est une tautologie pour tout Ψ et Ψ de F_0

équivalence
logique

référence
équivalence

équivalence
syntaxique

⚠ En général, en changeant de logique ou de langage, on ne pourra plus, \rightarrow systématiquement assurer cette propriété

Qu'est ce que l'équivalence ?

Parlons de relation binaires

* Une relation binaire R est un objet à deux arguments pour lequel on peut dire "x Ry est évalué" ou "x Ry n'est pas évalué"

Paradigme: • Formule logique:

On définit $x Ry$ à l'aide d'une formule $\Psi(x, y)$

Exemple: Considérons x, y de type de \mathbb{N} $x Ry$ lorsque $\exists n \in \mathbb{N} x = y + n$ (signifie $x > y$)

• Ensemble flottant

On définit R comme un ensemble de couples (x, y) d'éléments pris dans E ensemble pré-défini

$R \subseteq E \times E$
ensemble

Exemple: $\{x, y \in \mathbb{R}^2 / x^2 + y^2 = 1\}$ définition du cercle unité

• Entiers Binaires

On peut voir R comme une application $\prod_{E \times E} \rightarrow \{0, 1\}$ et associer $\prod_{E \times E} (x, y) = 1$ lorsque $x R y$.

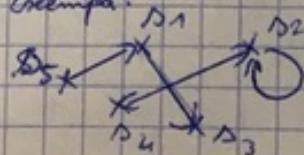
Exemple: $E = \{0, 1\} \rightarrow \{0, 1\}$

On pose $\text{1}_R(x, y) = x_1 \oplus x_2 \oplus \dots \oplus x_n \oplus y_1 \oplus y_2 \oplus \dots \oplus y_n$

• Graphes:

On peut considérer R comme un graphe G tel que s_1, s_2 forment une arête lorsque $s_1 R s_2$

Exemple:



Relation d'équivalence :

On dit que R est une relation d'équivalence sur E ou T . Considérons :

- R est une relation binaire.
- R vérifie les 3 contraintes

par exemple

- 1) Réflexivité : $\forall x \in E \quad xRx$
- 2) Symétrie : $\forall x \in E \forall y \in E \quad xRy \Rightarrow yRx$
- 3) Transitivité : $\forall x \in E \forall y \in E \forall z \in E \quad (xRy \wedge yRz) \Rightarrow xRz$

Exemples :

- l'égalité $=$ est une relation d'équivalence (particulière)

- $a \equiv b [n]$ notons \equiv_n la relation binaire sur \mathbb{Z} associée à \equiv_n est une relation d'équivalence.

Propriété : Sur F_0 , la relation \equiv est d'équivalence.

Démonstration :

1) Réflexivité : $\Phi \in F_0$ or $\Phi \equiv \Phi$ revient à $\Phi \subseteq \Phi$ (tautologie) d'où la réflexivité

2) Symétrie : $\Phi \equiv \Psi$ revient à $\Phi \rightarrow \Psi$ tautologie or $\Phi \rightarrow \Psi = (\Phi \rightarrow \Psi) \wedge (\Psi \rightarrow \Phi)$
 d'où $\Psi \equiv \Phi$

3) Transitivité : Supposons $\Phi \equiv \Psi$ et $\Psi \equiv \Sigma$

Par définition : pour Δ : $\sigma \rightarrow \{\text{vrai}, \text{faux}\}$
 on a $\|\Phi\|_\sigma = \|\Psi\|_\sigma$ et $\|\Psi\|_\sigma = \|\Sigma\|_\sigma$
 V étant quelconque on a $\Phi \equiv \Sigma$

Définition : Soit E muni de R relation d'équivalence, on définit pour $x \in E$ sa classe d'équivalence $\bar{x} = \{e \in E \mid eRx\}$
 (e autre relation avec x)

Exemple : sur \mathbb{Z} muni \equiv_n

$$(n=42) \quad \bar{3} = \{3, 45, 4203, 87, \dots\}$$

$$= \bar{3} + 42\mathbb{Z} = \bar{87}$$

Propriété : $xRy \Leftrightarrow \bar{x} = \bar{y}$

Vocabulaire : L'ensemble des classes \bar{x} d'équivalence sur E selon R est appelé ensemble quotient noté E/R .

$\mathbb{Z}/\equiv_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$ de cardinal $n \in \mathbb{N}^*$, $\bar{b} = b + n\mathbb{Z}$

en arithmétique, on favorise $\mathbb{Z}/n\mathbb{Z}$

Vision dans F_0 ~~$A > A \wedge A$~~ $A = A \wedge A$

Dans F_0/\equiv $\bar{A} = \bar{A} \wedge \bar{A}$

Notation : Δ soit un élément de σ

On écrit $\bar{A} = \alpha$ exemple : $\bar{A} = a = \bar{A} \wedge \bar{A}$
 Les opérations \wedge et \vee seront réécrites \times et $+$ dans cette structure.

⑥ Ainsi, dans \mathbb{F}_q , $a = \bar{a}a$; on écrit $1 = \bar{1}$ et $0 = \bar{1}$

Propriété: Soit $f: E \rightarrow F$ application

On définit $x R_f y$, par: $x R_f y (\Leftrightarrow f(x) = f(y))$
 R_f est une relation d'équivalence sur E .

Démonstration:

- 1) Reflexivité: Soit $x \in E$, $f(x) = f(x) \in F$ (l'application: $D_f = E$)
- 2) Symétrie: Supposons $x R_f y (\Leftrightarrow f(x) = f(y))$
- 3) Transitivité: Soient $(x; y; z) \in E^3$ tel que $x R_f y$ et $y R_f z$, on a donc $f(x) = f(y)$ et $f(y) = f(z)$
donc $f(x) = f(z)$

Exemple: Soient $M_n(\mathbb{C})$ ensemble des matrices carrées à coefficients complexes. On définit $A R B$ lorsque $\text{tr}({}^t \bar{A} A) = \text{tr}({}^t \bar{B} B)$, c'est une relation d'équivalence, $f: M_n(\mathbb{C}) \rightarrow \mathbb{C}$
 $x \mapsto \text{tr}({}^t \bar{x} x)$

($R = R_f$)

$A \sim B$ si et seulement si $a_{ii} = b_{ii}$

$\varphi: M_n(\mathbb{C}) \rightarrow \mathbb{C}^n$

$A \mapsto (a_{11}, \dots, a_{nn})$

On a $\varphi = R_f$: relation d'équivalence
 $\varphi^{-1} = \{ (a_{11}, \dots, a_{nn}) \}$

Généralisation: $\forall x \in E$ muni R_g d'équivalence $\bar{x} = f^{-1}(\{x\})$

Théorème: Il existe une correspondance bijective entre les relations d'équivalence sur E et les applications $f: E \rightarrow F$, $f(E)$ à préciser.

Démonstration: Il ne reste qu'à construire l'applications $R \mapsto f$.
On considère pour $x \in E$ l'ensemble \bar{x} fixé le même pour tous.
 $x \mapsto \bar{x} \mapsto x_0 \in \bar{x}$ fixe le même pour tous
 $E \rightarrow E/R \rightarrow F$

$$\begin{aligned} &= \text{relat} \rightarrow A = A \cap A \\ &A \text{ diff} \rightarrow E \neq F \end{aligned}$$

Exemple: $\Rightarrow x \mapsto \text{id}_E$

$f(x) = f(y) (\Leftrightarrow \text{id}(x) = \text{id}(y) (\Leftrightarrow x = y) \Leftrightarrow x R_f y)$

Définition: (Partition)

Soit Ω un ensemble. On dit que $(A_i)_{i \in I}$ est une partition de Ω lorsque:

$$\bigcup_{i \in I} A_i = \Omega$$

$$\forall i \neq j, A_i \cap A_j = \emptyset$$

Propriété: $\{f^{-1}(\{y\}); y \in F\}$ avec $f: E \rightarrow F$ forme une partition de E

$$g \in f^{-1}(\{y\}) \Leftrightarrow f(g) = y \quad (\text{D}_f = F)$$

Prenons y et y' distincts, posons $A_y = f^{-1}(y)$ et $A_{y'} = f^{-1}(y')$.

$x \in A_y \cap A_{y'}$, alors par définition, $y = f(x) = y'$ Absurde d'où $A_y \cap A_{y'} = \emptyset$

La logique classique:

Qu'est ce qui caractérise la logique classique?

Contradiction \neq Fausseté

- Le tiers exclu: "D'où une phrase, ou de sa négation, l'une est satisfaite"

- La non-nor élimination [Gödel]
"une double négation est une affirmation"

- La réciproce en question:

- L'équivalence:

Les trois règles caractéristiques se déduisent toutes d'une quelconque
Accepter une \Rightarrow Accepter les deux autres

- Les intuitionnistes:

Exclut le raisonnement par l'absurde et la tiers-exclusif (TE)
Initiation: Brouwer [1908]
"croire ce liberte à maïs"

- L'origine de la critique:

Pensez à l'existence de quelque chose

- Parole Brouwer!

Théorie du point fixe de Brouwer

Le cas intuitionniste

- L'algorithme au secours des intuitionnistes:

- Les quatre descriptions:

Turing: Les machines de Turing

Gödel: Les fonctions recursives

Rosch: Le Rekursiv - calcul

Bet:

- L'algorithme au secours des intuitionnistes:

- L'isomorphisme de Curry-Howard

- Le fragment logique

- Toute preuve intuitionniste est classique.

- Pouvoir déduire un inférieur

- Satisfaisabilité récursive - entre vrai et non-vrai

- Toute existence est constructive?

On ne peut que prouver l'existence en passant l'objet

- Toute solution est programmable

- Etudiable par la logique classique

Non auto-suffisant

II) La logique, c'est (aussi) Algébrique

Définition: (Monôde) Un ensemble E et $*$ construction à 2 arguments (loi de composition interne), on désigne par $(E; *)$ un monôde basiques:

- Associativité: $\forall x \forall y \forall z, (x * y) * z = x * (y * z)$

Polonais: $* x y z = * x * y z$

- Neutre: $\exists e \forall x, x * e = e * x = x$

Si c'est un groupe: - Inversibilité: $\forall x \exists y, x * y = y * x = e$

Si c'est un Abélien commutatif: $\forall x \forall y, x * y = y * x$

Exemple: $(\mathbb{N}; +)$ Monôde Groupe Abélien

$(\Sigma^*; \text{concat})$ Monôde Groupe Abélien (chiffre aléth)

(\mathbb{R}^*, \times) Monôde Groupe Abélien

$(\mathbb{Z}, +)$ Monoïde Groupe Abélien

$(C_{L^1}(\mathbb{R}), \circ)$ Monoïde Groupe Abélien

Un groupe est un monoïde.

Propriété : si l'élément "e" dont l'exemple est donné dans la définition est UNIQUE

↳ On le désigne par un symbole

Dans "inversibilité", si a_i est fixé, y associé est unique

↳ On le note a^{-1}

Langage des Groupes : \star symbole fonction à 2 arguments $\rightarrow \wedge \vee \Rightarrow (=)$ et

il est du e symbole de constante $\rightarrow \perp \top$

1 seule \neg symbole de fonction à 1 argument $\rightarrow \neg$

mais \sqrt{E} symbole de relation d'égalité $\rightarrow =$ [meta]

⚠ Ent...?

$$\Sigma = \{0, 1, 2, \dots, 9\}$$

$$\hookrightarrow (\Sigma^*, \text{concat}) \xrightarrow[\text{syntaxe}]{} (\mathbb{N}, +) \xrightarrow[\text{semantique}]{} \langle \omega_1, \omega_2 \rangle$$

Problème concaténation : $103 \quad 3452 \rightarrow 103 \quad 3452$

On l'ordonneur fait seulement des additions

$$\varphi: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

$$(n; k) \mapsto \varphi(n; k) = nk$$

$$\varphi(\varphi(n; m); k) = \varphi(n; \varphi(n; k))$$

$$\varphi(n; k) = n \times 10^{m+1} + k$$

Aspect calculatoire de la concaténation

Représentation / Vérification des groupes

\times	0	1	2	3	4	...	10
0	0	0	0	0	0	...	0
1	0	1	2	3	4	...	10
2	0	2	4	6	8	...	20
3	0	3	6	9	12	...	30
4	0	4	8	12	16	...	40
\vdots							
10	0						100

*	a	b	...	w
a	a	b	...	z
b	y	z	...	
\vdots				
w))))

Table de *

Gel } Suppressions doubles

$G = \text{cocardial}$

Définition : Soit $*$ un constructeur à deux arguments et G son domaine image.
On définit le tableau de $*$ pour la matrice T_\star .

$$T_\star(i, j) \rightarrow g_i * g_j \text{ où } G = \{g_1, \dots, g_n\}$$

On va tester « $(G, *)$ est un groupe » avec T_\star matrice carree d'ordre G .

Test 1 (interna/inversible)

$$\exists \forall i < |G| \exists \sigma = S_G, \exists T: S_G \left\{ \text{lign}_i(T_\star) = \sigma(G) \right. \\ \left. \text{et} \text{diag}_i(T_\star) = \tau(G) \right\}$$

$$\exists \exists p, q < |G| \text{ lign}_i(T_\star) = \text{col}_q; (T_\star)_i = \text{id}(G)$$

$$\exists \forall i \forall j \forall k (1 \leq i, j, k \leq |G|) \text{ avec } \varphi(a, b) = \text{index}((T_\star)_i a b)$$

$$T_\star(\varphi(i, j), k) = T_\star(\varphi(i, k), j)$$

Remarque: Il cause de l'histoïre, cet "anneau" en fait $\frac{1}{2}$ anneau le Boole et n'est donc plus un anneau au sens moderne.

Vocabulaire: On appelle anneau primitif noté $(A; +; \times)$ la structure Booleanne:

$$(F_0 / \equiv ; \bar{\vee} ; \bar{\wedge})$$

$\bar{\vee}$: classe d'équivalence de \vee $\bar{A} \bar{\vee} \bar{A} = \overline{A \vee A}$

Soit Δ une grande lettre.

On notera $\lambda = \overline{\Delta}$ sa classe d'équivalence dans F_0 . $A \vee A \neq \text{Identité}$
 $F_0 / \equiv = A \quad a \bar{\vee} a = a \quad \text{Identité}$
 $a + a = a$

Construisons de véritables anneaux de Boole:

• Soit \oplus défini comme $x \oplus y$

On a alors $(A; \oplus; \times)$ Anneau de Boole moderne

On définit sur $P(E)$ la différence symétrique notée Δ par:

$$A \Delta B = (A \cup B) \setminus (A \cap B) = (A \cup B) \cap (A \cap B)^c \quad x^c \text{ désigne } B \text{ complémentaire de } F$$

Exemple: Démontrer que $(P(E); \Delta)$ est un groupe

Indication: \emptyset est le neutre: $A \Delta \emptyset = (A \cup \emptyset) \cap (A \cap \emptyset)^c = A \cap (\emptyset)^c = A \cap E = A$

Structure (A, \oplus, \times)

Propriété: Toute équation polynomiale dans A est équivalente à une équation affine.

Démonstration: Provient de l'idendité: $x^n = x \Rightarrow \forall n \geq 2, x^n = x$, écrivons:

$$P = \sum_{k=0}^n \alpha_k x^k = \sum_{k=1}^n \alpha_k x + \alpha_0 = (\dots) \times x + \alpha_0$$

Généralise: Toute conjonction de contraintes dans A admet une représentation matricielle.

Propriété: $\bar{1}$ est neutre pour \times
 $\bar{1}$ est absorbant pour \times et neutre pour $+$ (ou \oplus) } dans A

Démonstration: Exercice

Notation: On écrit dans $\bar{1} = 1$ et $\bar{0} = 0$

Le problème SAT

On se donne $\Psi \in F_0$ s'écrivant sous la forme $\bigwedge_{i \in I} \bigvee_{j \in J} \alpha_{i,j} (P_{i,j})$

Notation: $\bigwedge_{i=1}^n \Psi_i = \Psi_1 \wedge \Psi_2 \wedge \Psi_3 \wedge \dots \wedge \Psi_n$ avec I et J finis et $\alpha_{i,j}$ soit ϕ soit \top

$$A = \bigcup_{i \in I} B_i$$

$$\Psi = \bigvee_{i \in I} B_i \text{ non fini}$$

SAT: Existe-t-il $\omega: \Omega \rightarrow \{\text{vrai}, \text{faux}\}$ telle que: $\|\Psi\|_\omega = \text{vrai}^9$?
si oui fournir ω
sinon, l'attester

A retenir: Problème NP-Complet

Vocabulaire: Si Ψ s'écrit $\bigwedge \bigvee \alpha_i (P_i)$, on dit que Ψ est une CNF (forme normale conjonctive)

Exemple: $(B_1 \wedge (B_2 \vee C)) \wedge (\neg B \vee A)$ où
 $\varphi_1 = \bigwedge_{i=1}^3 \varphi_i$

$$\varphi_1 = \bigvee_{j=1}^2 B_j \quad \text{dans } A \vee \neg$$

$$\varphi_2 = \bigvee_{j=1}^2 X_j \quad \text{avec } X_1 = B_3 \text{ et } X_2 = C$$

$$\varphi_3 = \bigvee_{j=1}^2 \alpha_j(Y_j) \quad \text{avec } \begin{cases} \alpha_1 = \top & Y_1 = B \\ \alpha_2 = \emptyset & Y_2 = A \end{cases}$$

Exemple: $(A \Rightarrow B) \wedge (\neg A \vee C)$ Non à cause de \Rightarrow
 $\equiv (\neg A \vee B) \wedge (\neg A \vee C)$ OUI

Théorème: Toute formule $\varphi \in F_0$ est sémantiquement équivalente à une CNF
 Δ Il n'y a jamais unicité

Démonstration: Par induction:

- Atomes, $T \perp$, tout $\Delta \in \cup$

$$\Delta \vdash T \quad \Delta \vdash \perp$$

- Construction: Si $\varphi = \bigwedge \alpha(P)$ et $\psi = \bigwedge \beta(Q)$
 On prouve que: $\varphi \wedge \psi \vdash \psi$ aussi

$$\frac{\varphi \vee \psi}{\Delta \vdash (\pi \sum \bar{\alpha}(p) + \tau \sum \beta(q))}$$

$$= \pi(\sum \sum \dots) = \pi(\sum \dots)$$

faitei
sous $\Delta \vdash \bigwedge \alpha(p)$ (lettres) idem

$$\left. \begin{array}{l} \varphi \Rightarrow \psi \equiv \neg \varphi \vee \psi \\ \varphi \Leftrightarrow \psi \equiv \neg(\varphi \oplus \psi) \\ \neg \varphi \rightarrow \gamma(\pi \sum \alpha(p)) \end{array} \right\}$$

$$A \vdash \pi(\sum \alpha(p))$$

Condition d'arrêt: W

→ D'après le Morgan, et ensuite regrouper les paquets.

Exemple Déterminer une CNF pour $\varphi = (A \Rightarrow x) \vee (B \wedge (\neg C \wedge A))$

notation: $\overline{A} = \bar{a}$

Demo A: $\overline{\varphi} = (\bar{a} + x) + (b \times (\bar{c} + a))$ comme un "univers" $(A; +; \times)$ et $(\bar{A}; \cdot; \times)$
 $= \bar{c} \times \bar{x} \times (b + (\bar{c} \times a))$ j'retourne à l'anneau
 $= \bar{c} \times b + \bar{c} \times (\bar{c} \times a)$
 $= (\bar{a} + x + b) \times (\bar{a} + x + \bar{c} + a)$

$$F_0: (\neg A \vee X \vee B) \wedge (\neg A \vee X \vee \neg C \vee A)$$

Définition: DNF pareil avec $\vee \wedge \alpha(P)$

Théorème: (version Dual)

Toute formule φ de F_0 possède une DNF.

Démonstration: Dualité des anneaux $(A; x, \times)$ et $(\bar{A}, \times, +)$ primitifs

Les Langages du Premier Ordre

On se donne ν à ceo près, que l'on remplace "majuscules" par "minuscules",
 $\nu = \{a; b; \dots; x; y; \dots; \alpha_{42}; \dots; \zeta_{127}\}$ infini dénombrables

L'ensemble de connecteurs

(neut) L'ensemble $\{\forall; \exists\}$ de quantificateurs

et enfin (neut) L₀ partie spécifique : - des symboles f₁, ..., f_n de fonctions munies de valeurs
 a_1, \dots, a_n nombre d'arguments respectifs.
 - des symboles R₁, ..., R_p de relations munies
 de valeur r₁, ..., r_p d'arité
 - des symboles de constantes C₁, ..., C_m

Exemple: On se donne L_{Cn} =

- O symbol de constante
- * symbol de fonction à 2 arguments
- (.) symbol de fonction à 1 argument
- ≡ symbol de relation d'arité 2

C'est le langage des groupes

* On se donne L_A =

- O symbol de constante
- 1 symbol de constante
- + symbol de fonction à 2 arguments
- X symbol de fonction à 2 arguments
- (-) symbol de fonction à 1 argument
- ≡ symbol d'une relation d'arité 2

C'est le langage des anneaux

Exemples: Langage des anneaux

$$\begin{array}{cccccc} O & 1 & + & \times & \equiv \\ \text{const} & \text{const} & \text{fct2} & \text{fct2} & \text{rel2} \\ & & \text{fonction à 2 arguments} & & \text{relation à 2 arguments} \end{array}$$

$(0+1)\times x + y$ est un terme $+x + 0 \ 1 \times y$ (idem en polynômes)

$1+1 \cancel{\times} 0 \quad 1+1 \cancel{\times} 2$ ne sont pas des termes à cause de =

~~$(\cancel{1}+\cancel{x})\cancel{\times} \cancel{1} + y$~~ n'est pas un terme car 2 n'est pas dans le langage

$$\begin{array}{c} L \\ \text{const} \\ \text{fct2} \\ \text{fct3} \end{array} \quad \begin{array}{c} \star \\ \text{fct2} \\ \text{3 arg} \end{array} \quad \begin{array}{c} \bowtie \\ \text{fct2} \\ \text{2 arg} \end{array} \quad \begin{array}{c} \boxtimes \\ \text{fct2} \\ \text{2 arg} \end{array}$$

$\nu: \text{Symbol} \rightarrow \text{arité (Symbol)} - 1$

$$\begin{array}{cccccccc} \star & \bowtie & x & \boxtimes & \star & \bowtie & L & R \\ \hline \nu & 1 & 2 & -1 & -1 & 1 & -1 & -1 & -1 \\ \hline \Sigma & 1 & 3 & 2 & 1 & 2 & 1 & 0 & \end{array}$$

À retenir: Un terme ne peut être construit avec un symbole de relation

(terme atomique)

Définition: Formules F_x(L) dites de 1^{er} ordre du langage L (par induction)

Si: atomiques, T et L et, pour tout symbole R_n de redaction d'arité n de L, si
 r_1, \dots, r_n sont n-termes, alors:

$P_1 \dots P_n$ est une formule atomique.

Θ: Si φ et ψ sont deux formules de $F_1(\mathcal{L})$

Alors $\varphi * \psi$ est une élément de $F_1(\alpha)$ avec $* \in \mathcal{L}$ à 2 args et aussi $\exists \forall$

De plus, si $\square \in \mathcal{U}$, notons $w = Q \square$ avec $Q \dots$

Si w n'apparaît pas déjà dans φ (en tant que mot), alors, $\forall w \varphi$ et $\exists w \varphi$ sont des formules de $F_1(\mathcal{L})$.

Condition d'arrêt: w

Exemple des \mathcal{L}_n :

$1 = 1$ formule atomique

$x + y = 0 \times 1$ formule atomique

$1 = 0 \Rightarrow x = 1$ formule non atomique

$\forall x \exists y x \equiv y \Rightarrow 1 = 1 \notin F_1(\mathcal{L})$

$\forall x \exists y x = y \Rightarrow 1 = 1 \in F_1(\mathcal{L})$ non atomique

Exemple: Langage choisi

Une formule atomique commence toujours par un symbole de relation.

• $\boxtimes \boxminus \boxstar \boxtimes \star x y \boxtimes k j l$ = $\oplus_{i=1}^n$
formule atomique

• $\forall x \exists y \boxtimes x y z t \Rightarrow \square$
formule non atomique

$\mathcal{L}_A \quad \forall x, \exists y, 1 = 0 \Rightarrow 1 \times x \equiv x$
terme constant forme usuelle

terme polynôme $\forall x x + x - 1 = 0 \Rightarrow x \times x \equiv x$
forme usuelle

terme polynôme $\forall x \Rightarrow x + x + 0 \equiv x \times x \equiv x$
forme usuelle

Polynôme $^2 \forall x \Rightarrow x + x + 0 \equiv x \times x \equiv x$

Satut des symboles de variables dans $F_1(\mathcal{L})$

Dans cette partie, $\varphi \in F_1(\mathcal{L})$ où est fixé. $\square \in \mathcal{U}$ quelconque.

• On dit que \square admet une occurrence dans φ lorsque \square apparaît en tant que symbole dans le mot φ .

exemples: $x + y = 0$ x admet une occurrence dans φ || y admet une occurrence dans φ || $=$ admet une occurrence dans φ || 0 n'a pas d'occurrence dans φ

Exemple 2: $\forall x_1 x_2 \exists x_3 + 0$ x_1 et x_2 ont une occurrence dans φ mais pas x lui-même

• Champ de quantification

Soit Q un quantificateur, tel que $Q \square$ apparaîsse dans φ (en tant que mot de deux symboles consécutifs).

Soit, φ la formule s'écrivant $s_1 \dots s_{i+n} \circ 0$

le champ de quantification de $Q \square$ dans φ est l'ensemble des indices i à $i+n$, on peut aussi adapter

La convention: \exists préquelle

champ de quantifi = {

Vocabulaire: une occurrence est liée.

libre hors champ lié dans un champ [de quantification]
(pour une même $\exists \in \{r\}$)

Définition: Un symbole φ est dit libre dans φ lorsque chaque occurrence l'est liée dans φ lorsque chaque occurrence l'est.

Exemple: Reprenons la formule: $x+1=0 \wedge x+y=0$ x est lié dans cette formule

Définition: φ est dite close lorsque chacun des symboles $\square \in \varphi$ admet au moins une occurrence dans φ est liée.

Exemple: La précédente n'est pas close.

$$\forall x \forall y \forall z ((x \times y) \times z = x \times (y \times z)) \quad A \times A \times A$$

L'axiome d'association est close

Procédure de construction:

Si φ contient \square dans un symbole de σ admettant au moins une occurrence liée, on se lance à un terme.

On écrit $\varphi[\square^t]$ désignant la formule φ obtenue en remplaçant chaque occurrence libre de \square dans φ par le terme t .

$$\varphi \text{ est } [\varphi/x] = y+1=0 \Rightarrow \exists x \quad x+y=0$$

Ainsi $\forall x \forall y \forall z \quad \varphi[\varphi/x]$ est close.

Vocabulaire: close φ c'est considérer $Q_1 \square_1 \dots Q_n \square_n$ en suffisamment

$Q_1 \square_1 \dots Q_n \square_n$ φ soit close (et bien construite)

Langages algébriques vs relationnels

Si L satisfait que \equiv d'entre 2 est symbole relationnel, on dit qu'il est algébrique.

Exemple: L'ensemble L Axioms L'algèbre $\left\{ \begin{array}{l} \Rightarrow \wedge \vee \Leftrightarrow \neg \\ \equiv \\ \leq \end{array} \right. \wedge \leq$ relation d'égalité

Exemples non Algébriques:

Relations d'ordre: $L = \left\{ \begin{array}{c} \equiv \\ \leq \\ \geq \end{array} \right. ; \frac{\leq}{2}$ relationnels

Avec pour contraintes à valider des: (ordres larges)

$A \times$ Reflexion $\forall x \quad x \leq x$

$A \times$ Anti-Symétrique $\forall x \forall y \quad x \leq y \wedge y \leq x \Rightarrow x = y$

$A \times$ Transitivité $\forall x \forall y \forall z \quad x \leq y \wedge y \leq z \Rightarrow x \leq z$

et aussi: réflexion = réécriture d'équivalence associée

⚠ L'équivalence n'est pas forcément l'égalité

Propriété supérieur : (total) $\forall x \forall y \exists z (x \leq y \wedge z \leq y \wedge x \equiv y \wedge z \equiv y)$

(P(C); =; \leq) ordre total
 (M; =; \leq) ordre total
 (T; =; \leq) ordre total
 A/B/C à dévisez entre exercice 17 et 18

(dense) $\forall x \forall y \exists z (x \leq y \wedge z \leq y \wedge x \equiv y \wedge z \neq y)$

Exemple: $(\mathbb{Q}, =, \leq)$ et $(\mathbb{R}; =; \leq)$ ordres denses
 $(\mathbb{Z}; =; \leq)$ - dense

Cas de l'égalité:

Schéma d'axiomatique de l'égalité : On dit que la relation d'équivalence \equiv est une égalité pour \mathcal{L} lorsque, quel que soit $\varphi \in F_{\mathcal{L}}(\mathcal{X})$
 admettant \Box pour variable libre, on a:
 $\forall u \forall v (u \equiv v \Rightarrow (\varphi[u/\Box] \Leftarrow \varphi[v/\Box])$ est une contrainte valide

Théorie: (pas au point)

On se donne un langage \mathcal{L} de 1^{er} ordre fixé. La donnée de formules closes en nombre fini ou
 enumerable par TM l'appelle théorie et ses éléments s'appellent
 Axiome.
 (Schéma d'axiomatique de la cas Turing Machine TM).

Exemple:

Le groupe : $e; *; (\cdot)^{-1}; \equiv$

Étude du groupe :

- A × A : $\forall x \forall y \forall z (x * y) * z \equiv x * (y * z)$
- A × unité
- A × d'inversibilité
- $(*) \equiv$ est d'égalité