Logique

Résumé des épisodes précédents

Des algorithmes qui construisent des démonstrations : démonstration automatique, théorème de Church

Des algorithmes qui opèrent sur des démonstrations : véfification des démonstrations, élimination des coupures

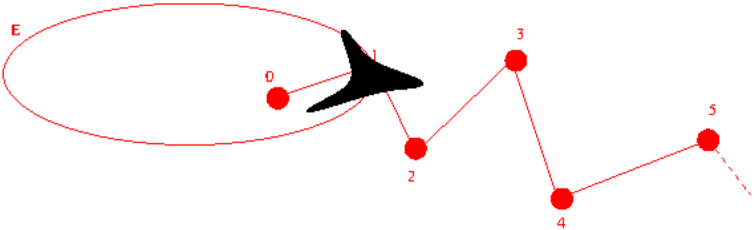
Des algorithmes qui remplacent des démonstrations : Presburger

La constructivité

Un autre type de relations entre démonstrations et algorithmes

Des démonstrations sont des algorithmes

Une question



Existe-il un entier n tel que $n \in E$ et $n+1 \notin E$?

Une démonstration de $\exists x \ A$

Mais pas de terme t tel que l'on ait une démonstration de $(t/x)A$

L'ensemble des propositions démontrables n'a pas la propriété du témoin

(si $\exists x \ A$ dans l'ensemble alors il existe un t tel que $(t/x)A$ aussi)

Mais comment cela est-il possible ?

Une seule manière de démontrer une proposition existentielle à partir d'une proposition sans quantificateur existentiel

$$\frac{\Gamma \vdash (t/x)A}{\Gamma \vdash \exists x \ A} \ \exists\text{-intro}$$

Dans notre exemple

P symbole de prédicat : $\Gamma = P(0), \neg P(S(S(0)))$

On ne peut pas démontrer $P(0) \wedge \neg P(S(0))$ $\quad (\hat{P}(0) = 1,\ \hat{P}(1) = 1,\ \hat{P}(2) = 0...)$

On ne peut pas démontrer $P(S(0)) \wedge \neg P(S(S(0)))$ $\quad (\hat{P}(0) = 1,\ \hat{P}(1) = 0,\ \hat{P}(2) = 0...)$

Mais on peut démontrer $\exists x\ (P(x) \wedge \neg P(S(x)))$

$$\dfrac{\dfrac{}{\Gamma \vdash P(S(0)) \vee \neg P(S(0))} \quad \dfrac{\dfrac{\dfrac{...}{}}{\Gamma, P(S(0)) \vdash P(S(0)) \wedge \neg P(S(S(0)))}}{\Gamma, P(S(0)) \vdash \exists x\ (P(x) \wedge \neg P(S(x)))} \quad \dfrac{\dfrac{...}{\Gamma, \neg P(S(0)) \vdash P(0) \wedge \neg P(S(0))}}{\Gamma, \neg P(S(0)) \vdash \exists x\ (P(x) \wedge \neg P(S(x)))}}{\Gamma \vdash \exists x\ (P(x) \wedge \neg P(S(x)))}$$

Un excès de témoins

Le responsable de la perte du témoin

$$\dfrac{\dfrac{}{\Gamma \vdash P(S(0)) \vee \neg P(S(0))} \quad \dfrac{\dfrac{\dots}{\Gamma, P(S(0)) \vdash P(S(0)) \wedge \neg P(S(S(0)))}}{\Gamma, P(S(0)) \vdash \exists x\ (P(x) \wedge \neg P(S(x)))} \quad \dfrac{\dfrac{\dots}{\Gamma, \neg P(S(0)) \vdash P(0) \wedge \neg P(S(0))}}{\Gamma, \neg P(S(0)) \vdash \exists x\ (P(x) \wedge \neg P(S(x)))}}{\Gamma \vdash \exists x\ (P(x) \wedge \neg P(S(x)))}$$

Le tiers exclu : ou bien $P(1)$ ou bien $\neg P(1)$, dans le premier cas 1 dans le second 0

Un exemple en mathématiques

$u_0 = \sqrt{2}$, $u_{n+1} = u_n^{\sqrt{2}}$
$E = \{n \mid u_n \text{ irrationnel}\}$

$0 \in E$, $2 \notin E$
Il existe n tel que $n \in E$ et $n+1 \notin E$
Donc il existe un irrationnel r tel que $r^{\sqrt{2}}$ rationnel

Ou bien $\sqrt{2}$ ou bien $\sqrt{2}^{\sqrt{2}}$ selon que $\sqrt{2}^{\sqrt{2}}$ est rationnel ou non

I. Les démonstrations constructives et la propriété du témoin

En déduction naturelle, on supprime la règle du tiers exclu

En calcul des séquents, on contraint les séquents à avoir une conclusion au plus

On garde (mais redémontre) l'équivalence entre la Déduction naturelle et le Calcul des séquents

On garde (mais redémontre) le théorème d'élimination des coupures

Du constructivisme à la constructivité

Une idée apparue dans un contexte polémique
Brouwer : les démonstrations qui utilisent le tiers exclu sont fausses
L'absence de fiabilité des principes logiques (1908)
Une des (nombreuses) crises de l'universalité de la vérité mathématique

Aujourd'hui : la crise est essentiellement résolue
Certaines démonstrations sont constructives et d'autres non

Mais encore des questionnements philosophiques (par exemple : la logique œcuménique)

La propriété de la dernière règle

Une démonstration dans le calcul des séquents

- constructive
- dans la théorie vide
- sans coupures

se termine par une règle logique à droite
(pas une contraction à droite, pas un axiome, pas une règle gauche, pas une coupure)

La propriété de la dernière règle

Une démonstration de $\exists x \; A$ dans le calcul des séquents

- constructive
- dans la théorie vide
- sans coupures

se termine par une règle $\exists$-droite

$$\dfrac{\dfrac{\cdots}{\vdash (t/x)A}}{\vdash \exists x\ A}\ \exists\text{-droite}$$

L'élimination des coupures

Si $\exists x\ A$ a une démonstration dans le calcul des séquents

- constructive
- dans la théorie vide

alors il existe un terme t tel que $(t/x)A$ soit démontrable

Le théorème

L'ensemble des propositions qui ont une démonstration constructive et dans la théorie vide a la propriété du témoin

Pour calculer le témoin : on élimine les coupures

S'étend à d'autres théories : l'arithmétique mais pas $\exists x\ P(x)$

II. Les modèles

Adieu la complétude ?

Si A valide dans tous les modèles de $\mathcal{T}$ alors A a une démonstration dans $\mathcal{T}$
~~Si A valide dans tous les modèles de $\mathcal{T}$ alors A a une démonstration constructive dans $\mathcal{T}$~~

Un problème de la logique constructive ou alors... de la notion de modèle

Adapter la notion de modèle : les modèles de Kripke et les modèles de Heyting
Deux solutions, mais un certain nombre de points en commun

Le meilleur des mondes possibles

La proposition « Il y a à Paris une tour haute de 324 m » est vraie
Mais nous pouvons imaginer un monde possible (Leibniz) dans lequel elle est fausse

La proposition $\neg\exists x\ (x + 1 = 0)$ est valide dans le modèle $\mathbb{N}$
Mais il y a des modèles dans lesquels elle n'est pas valide

Unique symbole P, prédicat sans argument, $\neg P$ est valide dans le modèle $\mathcal{M}_3$ ($\hat{P} = 0$)
Mais pas dans le modèle $\mathcal{M}_4$ ($\hat{P} = 1$)

Non un modèle, mais plusieurs

Utile pour modéliser : la contingence (il pleut, mais il pourrait ne pas pleuvoir), le temps (il pleut aujourd'hui, mais demain il ne pleuvra pas), la connaissance (je ne sais pas s'il pleut ou non) et... la constructivité

Les modèles de Kripke

- Une famille de modèles classiques (pour éviter la confusion, chacun est appelé « un monde »)
- une relation réflexive et transitive $\preceq$ sur les mondes : $w \preceq w'$, w' est après w
- tels que si $w \preceq w'$ alors $\mathcal{M}_s^w \subseteq \mathcal{M}_s^{w'}$, $\hat{f}^w \subseteq \hat{f}^{w'}$
  et si $\hat{P}^w(a_1, ..., a_n) = 1$ alors $\hat{P}^{w'}(a_1, ..., a_n) = 1$

Si A n'est pas valide en w, A n'est pas nécessairement fausse : A est peut-être vraie mais on ne le sait pas encore en w

L'interprétation d'une proposition dans un monde

$[\![A]\!]_\phi^w$ ne dépend pas uniquement de w mais aussi des mondes dans le futur de w

- $[\![P(t_1, ..., t_n)]\!]_\phi^w = \hat{P}([\![t_1]\!]_\phi^w, ..., [\![t_n]\!]_\phi^w)$
- $[\![\top]\!]_\phi^w = 1$
- $[\![\bot]\!]_\phi^w = 0$
- $[\![A \wedge B]\!]_\phi^w = 1$ si $[\![A]\!]_\phi^w = 1$ et $[\![B]\!]_\phi^w = 1$, 0 sinon
- $[\![A \vee B]\!]_\phi^w = 1$ si $[\![A]\!]_\phi^w = 1$ ou $[\![B]\!]_\phi^w = 1$, 0 sinon
- $[\![\exists x\ A]\!]_\phi^w = 1$ s'il existe $a \in \mathcal{M}^w$ tel que $[\![A]\!]_{\phi, x=a}^w = 1$, 0 sinon
- $[\![A \Rightarrow B]\!]_\phi^w = 1$ si pour tout $w' \succeq w$, si $[\![A]\!]_\phi^{w'} = 1$ alors $[\![B]\!]_\phi^{w'} = 1$, 0 sinon
- $[\![\neg A]\!]_\phi^w = 1$ si pour tout $w' \succeq w$, $[\![A]\!]_\phi^{w'} = 0$, 0 sinon
- $[\![\forall x\ A]\!]_\phi^w = 1$ si pour tout $w' \succeq w$, et pour tout a dans $\mathcal{M}^{w'}$, $[\![A]\!]_{\phi, x=a}^{w'} = 1$, 0 sinon

La définition de la validité dans un modèle de Kripke

A est valide dans le monde w si pour toute valuation ϕ à valeur dans $\mathcal{M}^w$, $[\![A]\!]_\phi^w = 1$
A est valide dans le modèle si A valide dans tous les mondes

Nouveaux théorèmes de correction et de complétude

Un exemple de modèle où le tiers exclu n'est pas valide

Un langage avec un unique symbole P, prédicat sans argument

Deux mondes : w_3 ($\hat{P}^{w_3} = 0$) et w_4 ($\hat{P}^{w_4} = 1$)
$w_3 \preceq w_4$

$[\![P]\!]^{w_3} = \hat{P}^{w_3} = 0$
$[\![\neg P]\!]^{w_3} = 0$, car $w_4 \succeq w_3$ et $[\![P]\!]^{w_4} = 1$
$[\![P \vee \neg P]\!]^{w_3} = 0$

Les modèles de Heyting

Un monde peut se définir comme un ensemble de faits (les faits qui y sont vrais)
Mais un fait peut se définir comme un ensemble de mondes (les mondes où il est vrai)

$[\![A]\!] = 0$ ou $1 \longrightarrow [\![A]\!] =$ l'ensemble des mondes où A est vraie

Les modèles de la contingence

Un langage avec un unique symbole P, prédicat sans argument
Deux modèles : $\mathcal{M}_3 : \hat{P} = 0$ et $\mathcal{M}_4 : \hat{P} = 1$

Un nouveau modèle dans lequel
$[\![A]\!]_\phi$ est l'ensemble des i tels que $[\![A]\!]_\phi = 1$ dans $\mathcal{M}_i$
$[\![P]\!] = \{4\}$, $[\![\neg P]\!] = \{3\}$, $[\![P \wedge \neg P]\!] = \varnothing$, $[\![P \vee \neg P]\!] = \{3, 4\}$

$[\![A]\!]_\phi$ est un élément de $\mathcal{P}(\{3, 4\})$ (quatre valeurs de vérité, pas bi-valué)
$[\![A \wedge B]\!]_\phi$ est l'intersection de $[\![A]\!]_\phi$ et $[\![B]\!]_\phi$
$[\![\forall x\ A]\!]_\phi$ est l'intersection de tous les ensembles $[\![A]\!]_{\phi, x=a}$
$[\![A \vee B]\!]_\phi$ est la réunion de $[\![A]\!]_\phi$ et $[\![B]\!]_\phi$
$[\![A \Rightarrow B]\!]_\phi$ est $(\{3, 4\} \setminus [\![A]\!]_\phi) \cup [\![B]\!]_\phi$
...
A valide si pour tout ϕ, $[\![A]\!]_\phi = \{3, 4\}$

Un cas particulier des algèbres de Boole

$\langle \mathcal{B}, \leq, \hat{\top}, \hat{\bot}, \hat{\neg}, \hat{\wedge}, \hat{\vee}, \hat{\Rightarrow}, \hat{\forall}, \hat{\exists} \rangle$
$\mathcal{B}$ un ensemble, $\leq$ une relation sur $\mathcal{B}$, $\hat{\top}$ et $\hat{\bot}$ éléments de $\mathcal{B}$, $\hat{\neg}$ fonction de $\mathcal{B}$ dans $\mathcal{B}$, $\hat{\wedge}$, $\hat{\vee}$ et $\hat{\Rightarrow}$ fonctions de $\mathcal{B} \times \mathcal{B}$ dans $\mathcal{B}$, $\hat{\forall}$ et $\hat{\exists}$ fonctions (partielle) de $\mathcal{P}(\mathcal{B})$ dans $\mathcal{B}$
tels que

- $\leq$ relation d'ordre
- $\hat{\top}$, $a \mathbin{\hat{\wedge}} b$ et $\hat{\forall}\, E$ bornes inférieures de $\varnothing$, $\{a, b\}$, E
- $\hat{\bot}$, $a \mathbin{\hat{\vee}} b$ et $\hat{\exists}\, E$ bornes supérieures de $\varnothing$, $\{a, b\}$, E
- $\hat{\neg}\, a = (a \mathbin{\hat{\Rightarrow}} \hat{\bot})$
- $a \leq b \mathbin{\hat{\Rightarrow}} c$ si et seulement si $a \mathbin{\hat{\wedge}} b \leq c$
- $b \mathbin{\hat{\vee}} (b \mathbin{\hat{\Rightarrow}} c) = \hat{\top}$

De nouveaux théorèmes de correction et complétude

Un nouveau théorème de correction

> Si A démontrable dans $\mathcal{T}$, alors A valide dans tous les modèles (valués dans une algèbre de Boole) de $\mathcal{T}$

Récurrence sur la structure des démonstrations

Le théorème de complétude

> Si A valide dans tous les modèles (valués dans une algèbre de Boole) de $\mathcal{T}$, alors A démontrable dans $\mathcal{T}$

corollaire du théorème de complétude pour les modèles bi-valués, puisque $\{0, 1\}$ est une algèbre de Boole parmi d'autres

Quel rapport avec la constructivité ?

Le tiers exclu est valide dans tous les modèles valués dans une algèbre de Boole
Mais on peut étendre la définition

- $\leq$ relation d'ordre
- $\hat{\top}$, $a \mathbin{\hat{\wedge}} b$ et $\hat{\forall}\ E$ bornes inférieures de $\varnothing$, $\{a, b\}$, E
- $\hat{\bot}$, $a \mathbin{\hat{\vee}} b$ et $\hat{\exists}\ E$ bornes supérieures de $\varnothing$, $\{a, b\}$, E
- $\hat{\neg}\ a = (a \mathbin{\hat{\Rightarrow}} \hat{\bot})$
- $a \leq b \mathbin{\hat{\Rightarrow}} c$ si et seulement si $a \mathbin{\hat{\wedge}} b \leq c$
- $\cancel{b \mathbin{\hat{\vee}} (b \mathbin{\hat{\Rightarrow}} c) = \hat{\top}}$

Une algèbre de Heyting
Nouveaux théorèmes de correction et de complétude

Un exemple de modèle où le tiers exclu n'est pas valide

$\mathcal{B}$ est l'ensemble des ouverts de $\mathbb{R}$

La réunion d'ouverts est un ouvert ($\hat{\perp}$, $\hat{\vee}$, $\hat{\exists}$)
L'intersection finie d'ouverts est un ouvert ($\hat{\top}$, $\hat{\wedge}$)
Mais pas l'intersection infinie ($\hat{\forall}$) ni le complémentaire ($\hat{\Rightarrow}$, $\hat{\neg}$) : dans ce cas

$$a \mathrel{\hat{\Rightarrow}} b = \overset{\circ}{\widehat{\mathbb{R} \setminus a}} \cup b$$

$$\hat{\neg}\, a = \overset{\circ}{\widehat{\mathbb{R} \setminus a}}$$

Un langage avec un unique symbole P, prédicat sans argument
$\hat{P} = \{x \in \mathbb{R} \mid x > 0\}$
$[\![\neg P]\!] = \{x \in \mathbb{R} \mid x < 0\}$
$[\![P \vee \neg P]\!] = \mathbb{R} \setminus \{0\} \neq \mathbb{R}$

III. Programmer avec des démonstrations

Dans l'arithmétique, la proposition

$$\forall x \exists y \ (x = 2 \times y \vee x = 2 \times y + 1)$$

a une démonstration constructive (récurrence sur x)
Et

$$\exists y \ (25 = 2 \times y \vee 25 = 2 \times y + 1)$$

aussi

Comment calcule-t-on le témoin ?

Quel est-il ?

Les démonstrations sont des programmes

Une démonstration (constructive) de

$$\forall x \exists y \ (x = 2 \times y \vee x = 2 \times y + 1)$$

est un programme qui calcule la moitié

Son mécanisme d'exécution est l'élimination des coupures

Il est correct vis à vis de la spécification

$$x = 2 \times y \vee x = 2 \times y + 1$$

Les démonstrations constructives en mathématiques

Analyse constructive : analyse numérique

Algèbre constructive : calcul formel

De la constructivité à l'œcuménisme (rappelez-vous la logique martienne)

Les règles de déduction définissent la signification des symboles logiques $\wedge, \vee$...
Règles différentes : signification différente
Signification différente : notation différente : $\vee$, $\vee_c$ (comme on avait déjà $\vee$ et $\oplus$)

$\exists_c$ = il existe, $\exists$ = on connaît

$\vee$ et $\vee_c$ peuvent cohabiter dans la même logique : logique œcuménique

Dans la théorie vide $P \vee \neg P$ n'est pas démontrable, mais $P \vee_c \neg P$ si

La constructivité n'est pas une propriété des démonstrations, mais des symboles logiques

La crise du constructivisme : un malentendu ?

La prochaine fois

La Résolution