Logique

Résumé des épisodes précédents

Une fusée à deux étages :
logique ($\Rightarrow$, $\forall$...)
théorie ($=$, $+$, $\times$, $\in$...)

Exemples de théories : PA...

Démontrabilité dans PA indécidable
Démontrabilité dans la logique des prédicats indécidable (théorème de Church)

Des théories décidables

De l'utilisation positive des résultats négatifs

- Le théorème de Church demande un prédicat binaire : si que des prédicats unaires décidable
- La démontrabilité peut devenir décidable si on ajoute des axiomes : identifier des théories décidables : Presburger, Skolem, Tarski...

Comment montrer qu'une théorie est décidable ?

(Parmi d'autres) deux méthodes

Si A non démontrable dans $\mathcal{T}$, alors il existe un modèle fini de $\mathcal{T}, \neg A$
Énumération des démonstrations et des modèles finis

Décidabilité de la démontrabilité des propositions closes sans quantificateurs
Élimination des quantificateurs

I. La méthode du modèle fini

Un unique symbole de prédicat unaire

Décidabilité de la théorie vide avec un unique symbole de prédicat unaire P

$\forall x\ P(x)$, $\exists x\ P(x)$, $\exists x\ (P(x) \Rightarrow \forall y\ P(y))$...

Un modèle $\mathcal{M}$ de cardinal quelconque, deux genres d'objets : les a tels que $\hat{P}(a) = 1$ et ceux tels que $\hat{P}(a) = 0$
Tous les a tels que $\hat{P}(a) = 1$ sont indiscernables (idem pour ceux tels que $\hat{P}(a) = 0$)
On quotiente par la relation $a \sim b$ ssi $\hat{P}(a) = \hat{P}(b)$
Un modèle de cardinal 1 ou 2 qui valide les mêmes propositions que $\mathcal{M}$

Un unique symbole de prédicat unaire

Si A non démontrable alors il existe un modèle fini de $\neg A$: énumération des démonstrations et des modèles finis

A démontrable ssi A valide dans tous les modèles ssi A valide dans tous les modèles de cardinal ≤ 2

Généralisation à n symboles de prédicats unaires (2^n)

II. L'élimination des quantificateurs

L'élimination des quantificateurs

$A \mapsto A'$
A' sans quantificateurs
$A \Leftrightarrow A'$ démontrable

Le cas où A est de la forme $\exists x\ B$ ou $\forall x\ B$ avec B sans quantificateurs suffit (récurrence)
Le cas où A est de la forme $\exists x\ B$ avec B sans quantificateurs suffit
Si $(\exists x\ \neg B) \Leftrightarrow C'$ alors $(\forall x\ B) \Leftrightarrow (\neg \exists x \neg B) \Leftrightarrow (\neg C')$

L'exemple le plus célèbre

$$\exists x\ (ax^2 + bx + c = 0)$$

$$\Leftrightarrow$$

$$((\neg a = 0 \wedge b^2 - 4ac \geq 0) \vee (a = 0 \wedge (\neg b = 0 \vee c = 0)))$$

Trois exemples : les ordres totaux denses sans extrémités, l'arithmétique de Presburger, l'analyse élémentaire

III. La théorie des ordres totaux denses sans extrémités

Les axiomes

$=, <$

Axiomes de l'égalité
Ordre strict : antiréflexivité, transitivité

Total :

$$\forall x \forall y \ (x < y \vee y < x \vee x = y)$$

Dense :

$$\forall x \forall y \exists z \ (x < y \Rightarrow (x < z \wedge z < y))$$

Sans extrémités :

$$\forall x \exists y \ (y < x)$$

$$\forall x \exists y \ (x < y)$$

Un exemple

Équivalence des propositions

$$\exists x\ (y < x \land x < z \land x < z')$$

$$y < z \land y < z'$$

Le cas général : étape 1

On supprime les implications

$$C \Rightarrow D \longrightarrow \neg C \vee D$$

On supprime les négations

$$\neg(C \vee D) \longrightarrow \neg C \wedge \neg D$$

$$\dots$$

$$\neg(y < z) \longrightarrow (z < y \vee z = y)$$

$$\neg(y = z) \longrightarrow (y < z \vee z < y)$$

On distribue $\wedge$ sur $\vee$
On simplifie $\top$ et $\bot$

$$\top \wedge C \longrightarrow C \quad \bot \wedge C \longrightarrow \bot \quad \top \vee C \longrightarrow \top \quad \bot \vee C \longrightarrow C$$

Forme normale disjonctive : disjonction de conjonctions de propositions atomiques (ou $\top$ ou $\bot$)

Le cas général : étape 1

On distribue $\exists$ sur $\vee$

$$\exists x\ (C \vee D) \longrightarrow (\exists x\ C \vee \exists x\ D)$$

$\exists x\ A$ avec A conjonction de propositions atomiques
On sort les propositions atomiques D qui ne contiennent pas x

$$\exists x\ (C \wedge D) \longrightarrow (\exists x\ C) \wedge D$$

On supprime les $x = y$, $y = x$, $x = x$ et $x < x$

$$\exists x\ (x = y \wedge C) \longrightarrow (y/x)C$$

$$\exists x\ (x = x \wedge C) \longrightarrow \exists x\ C$$

$$\exists x\ (x < x \wedge C) \longrightarrow \bot$$

$\exists x\ A$ avec A conjonctions de propositions de la forme $x < y$ ou $y < x$

Le cas général : étape 2

$$\exists x \ ((\bigwedge_{y \in I} y < x) \wedge (\bigwedge_{z \in J} x < z))$$

Si I et J non vides

Un point entre le maximum des y et le minimum des z :

$$\bigwedge_{y \in I, z \in J} (y < z)$$

(densité)

Si I vide ou J vide $\top$ (pas d'extrémités)

IV. L'arithmétique de Presburger

Le théorème de Presburger

L'ensemble des propositions formées dans le langage 0, S, $+$, $=$ et valides dans le modèle $\mathbb{N}$ est décidable

Attention : pas « démontrables dans l'arithmétique de Presburger » (Corollaire ?)

Chaque proposition en axiome : théorie axiomatique cohérente, complète et décidable

Un autre critère de vérité pour les propositions linéaires : le calcul remplace la démonstration

Corollaire d'un théorème plus simple

Ensemble des propositions formées dans le langage 0, 1, $+$, $\leq$, $-$, $Mult_2$, $Mult_3$, $Mult_4$...

valides dans le modèle $\mathbb{Z}$

décidable

Validité des propositions closes et sans quantificateurs

Trivialement décidable

$$4 + 5 \leq 8 \vee \mathit{Mult}_4(7)$$

Un exemple

$$\exists x \ (1 \leq 3.x \wedge x \leq 7 - x) \ ?$$

On rassemble les x d'un coté et les autres termes de l'autre

$$\exists x \ (1 \leq 3.x \wedge 2.x \leq 7)$$

On multiplie la première inéquation par 2 et la seconde par 3

$$\exists x \ (2 \leq 6.x \wedge 6.x \leq 21)$$

On effectue un changement de variable

$$\exists x' \ (2 \leq x' \wedge x' \leq 21 \wedge Mult_6(x'))$$

Existe-t-il un multiple de 6 dans l'intervalle 2..21 ? Oui : 18

Les variables libres : un autre exemple

$$\exists x \ (1 \leq 3.x \wedge x \leq y - x)$$

On rassemble les x d'un coté et les autres termes de l'autre

$$\exists x \ (1 \leq 3.x \wedge 2.x \leq y)$$

On multiplie la première inéquation par 2 et la seconde par 3

$$\exists x \ (2 \leq 6.x \wedge 6.x \leq 3.y)$$

On effectue un changement de variable

$$\exists x \ (2 \leq x \wedge x \leq 3.y \wedge Mult_6(x))$$

Existe-t-il un multiple de 6 dans l'intervalle $2..3.y$?

Les variables libres : un autre exemple

S'il en existe un alors le plus grand est $3.y$, $3.y-1$, $3.y-2$, $3.y-3$, $3.y-4$ ou $3.y-5$

$\exists x \ A$ équivalent à

$$(3y/x)A \vee (3y-1/x)A \vee (3y-2/x)A \vee (3y-3/x)A \vee (3y-4/x)A \vee (3y-5/x)A$$

qui est sans quantificateurs

Des inéquations $x \leq t$: on accroche une solution à l'un des t (ici $3.y$)

Mais si pas d'inéquations...

$$\exists x\ (2 \leq x \wedge Mult_6(x))$$

S'il y a une solution p tous les p' supérieurs à p et congrus à p modulo 6 sont aussi solution

$$\exists x\ (\top \wedge Mult_6(x))$$

Périodique de période 6 et coïncide avec $\exists x\ A$ à partir d'un certain rang
La tester sur une période

$$(0/x)A' \vee (1/x)A' \vee (2/x)A' \vee (3/x)A' \vee (4/x)A' \vee (5/x)A'$$

Sans quantificateurs

Le cas général : étape 1

Proposition $\exists x\ A$, A sans quantificateurs
On supprime les implications

$$C \Rightarrow D \longrightarrow \neg C \vee D$$

On supprime les négations

$$\neg(C \vee D) \longrightarrow \neg C \wedge \neg D$$

$$...$$

$$\neg t \leq u \longrightarrow u + 1 \leq t$$

$$\neg Mult_n(t) \longrightarrow Mult_n(t+1) \vee ... \vee Mult_n(t+n-1)$$

Une proposition formée avec $\top$, $\bot$, $\wedge$, $\vee$ à partir de propositions atomiques de la forme $t \leq u$ ou $Mult_n(t)$

Le cas général : étape 2

Dans chaque inéquation, les x d'un coté du signe $\leq$ et les autres termes de l'autre
On multiplie pour égaliser les coefficients
On effectue un changement de variable

Une proposition formée avec les mêmes connecteurs à partir de propositions atomiques de la forme
$x \leq t$, $t \leq x$, $0 \leq t$, $Mult_n(x+t)$ et $Mult_n(t)$
où t est un terme qui ne contient pas x
(Pour chaque valuation ρ), périodique de période r à partir d'un certain rang

Le cas général : étape 3

E ensemble de tous les t tels que $x \leq t$ apparaisse dans A
A' obtenue en remplaçant dans A les propositions de la forme $x \leq t$ par $\perp$ et les propositions de la forme $t \leq x$ par $\top$ (périodique et coïncide avec A à partir d'un certain rang)

B disjonction de toutes les propositions de la forme

- $((t-j)/x)A$ où t terme de E et j entier compris entre 0 et $r-1$
- $(i/x)A'$ où i entier compris entre 0 et $r-1$

Le cas général : étape 3

- $((t-j)/x)A$ où t terme de E et j entier compris entre 0 et $r-1$
- $(i/x)A'$ où i entier compris entre 0 et $r-1$

$\exists x\ A$ valide ssi B valide
Pour chaque valuation ρ et solution p deux cas possibles
(1) tous les p' supérieurs à p et congrus à p modulo r solutions
(2) ce n'est pas le cas
Dans le premier cas l'un des $(i/x)A'$ est valide
Dans le second l'un des $((t-j)/x)A$ est valide

Réciproque triviale

Donc

L'arithmétique de Presburger est décidable

Corollaire : $\times$ n'est pas définissable dans l'arithmétique de Presburger
Corollaire : l'existence de solutions entières à des inéquations linéaires est décidable

V. Décidabilité de l’analyse élémentaire (Tarski)

Ensemble des propositions formées dans le langage $+$, $\times$, $=$, $<$ et valides dans $\mathbb{R}$ décidable

$$\exists x \ (ax^2 + bx + c = 0)$$

$$\Leftrightarrow$$

$$((\neg a = 0 \wedge b^2 - 4ac \geq 0) \vee (a = 0 \wedge (\neg b = 0 \vee c = 0)))$$

Géométrie élémentaire décidable

La prochaine fois

Retour sur le tiers exclu : la notion de démonstration constructive