Conséquences de l'incomplétude de l'arithmétique

Des théories décidables

0. Résumé des épisodes précédents

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

Cohérence / contradiction
Complétude / incomplétude
Décidabilité / indécidabilité

Exemples de théories

PA indécidable et incomplète

Aujourd'hui : conséquences de l'incomplétude de PA, des théories décidables

I. Conséquences de l'incomplétude de l'arithmétique

Exercice

Montrer qu'il existe une proposition A valide dans $\mathbb{N}$ mais non démontrable dans l'arithmétique
Montrer $PA, \neg A$ cohérente
Montrer $PA, \neg A$ a un modèle $\mathcal{M}$
Montrer que $\mathcal{M}$ et $\mathbb{N}$ valident des propositions différentes

Modèle non standard de l'arithmétique

Typiquement

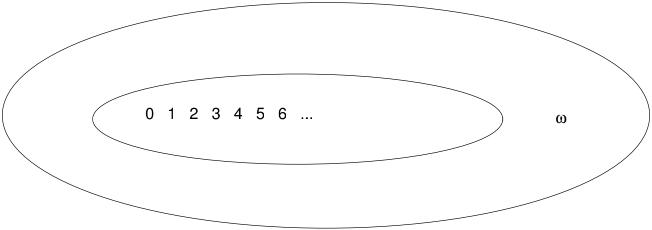
$$A = \neg\exists x_1 ... \exists x_n \ (t = u)$$

L'équation polynomiale $t = u$ n'a pas de solution dans $\mathbb{N}$ mais cela ne peut pas se démontrer dans PA

$\mathcal{M}$ contient des objets qui sont solutions de l'équation polynomiale : ce ne sont pas des entiers

La faiblesse du schéma de compréhension

$$\forall c\ (0 \epsilon c \Rightarrow \forall x\ (x \epsilon c \Rightarrow S(x) \epsilon c) \Rightarrow \forall y\ y \epsilon c)$$



$$\overline{\forall}\ \exists c \forall z\ (z \epsilon c \Leftrightarrow A)$$

N'énonce que l'existence des classes définissables
Les classes qui contiennent 0, 1, 2... mais par ω ne sont pas définissables

Un entier infini

Lowenheim-Skolem : PA a un modèle non dénombrable
Démonstration : ensemble non dénombrable de constantes
$PA \cup \{c \neq c' \mid c \neq c'\}$ a un modèle

Exercice :
Une constante ω
Montrer $PA \cup \{\omega \neq 0, \omega \neq 1, \omega \neq 2, ...\}$ a un modèle
Montrer que l'interprétation ω de ω n'est pas un entier

idem $PA \cup \{\omega \geq 0, \omega \geq 1, \omega \geq 2, ...\}$

La résurrection des infinitésimaux

Exercice :
Une constante ε
Un théorie cohérente $\mathcal{T}$ où l'on parle des réels (par exemple ZF)
Montrer $\mathcal{T} \cup \{\varepsilon \in \mathbb{R}, \varepsilon > 0, \varepsilon \leq 1, \varepsilon \leq 1/2, \varepsilon \leq 1/3, ...\}$ a un modèle

Analyse non standard

Une construction de ε

μ fonction de $\mathcal{P}(\mathbb{N})$ dans $\{0, 1\}$ t.q.
$\mu(\mathbb{N}) = 1$
$\mu(X) = 0$ si X fini
si X et Y disjoints, alors $\mu(X \cup Y) = \mu(X) + \mu(Y)$

Relation d'équivalence sur les suites de réels
$u \sim v$ ssi $\mu(\{i \mid u_i = v_i\}) = 1$
${}^*\mathbb{R}$: $(\mathbb{N} \to \mathbb{R})/\sim$

injection de $\mathbb{R}$ dans ${}^*\mathbb{R}$: $r, r, r, r, r, \ldots$
mais $\varepsilon = (1/n)_n/\sim$

Même propriétés (exprimables) que les réels

II. Des théories décidables

De l'utilisation positive des résultats négatifs

Le théorème de Church : logique des prédicats indécidable

Mais

1. demande un prédicat binaire : si que des prédicats unaires décidable
2. semi-décidable : méthodes de démonstration automatique
3. peut devenir décidable si on ajouter des axiomes : identifier des théories décidables Presburger, Skolem, Tarski, ...

Comment montrer qu'une théorie est décidable ?

(Parmi d'autres) deux méthodes

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

Décidabilité des propositions sans quantificateurs
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

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

$$\Leftrightarrow$$

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

Aujourd'hui : trois exemples : les ordres denses sans extrémités, l'arithmétique de Pressburger, 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

Exercice :
Montrer l'équivalence des propositions

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

$$y < z \wedge y < z'$$

Le cas général : étape 1

On supprime les implications

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

On supprime les négations

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

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

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

On distribue $\wedge$ sur $\vee$ (forme normale disjonctive)
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

Le cas général : étape 2

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 3

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

Si I vide ou J vide $\top$ (pas d'extrémités)
Sinon un point entre le maximum des y et le minimum des z :

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

(densité)

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 PA » Équivalence ?

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

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

Un théorème plus simple et équivalent

Ensemble des propositions formées dans le langage 0, 1, $+$, $\leq$, $-$, *Mult*$_2$, *Mult*$_3$, *Mult*$_4$, ...

valides dans le modèle $\mathbb{Z}$

décidable

Un théorème plus simple et équivalent

Validité des propositions closes et sans quantificateurs trivialement décidables

$$4 + 5 \leq 8 \vee Mult_4(7)$$

Il suffit de montrer l'élimination du quantificateur existentiel
car $\forall x\ B$ valide ssi $\neg \exists x \neg B$ valide ssi $\exists x \neg B$ non valide

Un problème de décision de l'existence de solutions entières à des inéquations linéaires

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

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

Multiple de 6 dans l'intervalle 2..21 : oui

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

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

Les variables libres : un autre exemple

Pour chaque valeur q de y et solution p : deux cas possibles

(1) tous les p' supérieurs à p et congrus à p modulo 6 solutions

(2) ce n'est pas le cas
Alors il existe p' solution t.q. $p' + 6$ ne soit pas solution
Une inéquation $(x' \leq 3.y)$ change d'avis entre p' et $p' + 6$.
$p' \leq 3.q < p' + 6$
il existe j compris entre 0 et 5 tel que $p' + j = 3.q$: $p' = 3.q - j$
Il existe une solution de la forme $3.q - j$
$(3.y/x')A' \vee ((3.y-1)/x')A' \vee ((3.y-2)/x')A' \vee ((3.y-3)/x')A' \vee ((3.y-4)/x')A' \vee ((3.y-5)/x')A'$

Le cas général : étape 1

Proposition 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
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
Périodique 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 $\top$ (coïncide avec A pour les grandes valeurs, périodique)

B disjonction de toutes les propositions de la forme

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

Le cas général : étape 3

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

$\exists x\ A$ valide ssi B valide
Pour chaque valeur $q_1, ..., q_n$ des variables libres de $\exists x\ A$ 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

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

Un défi

Intégrer ces méthodes à des programmes de démonstration automatique

La prochaine fois

La démonstration automatique