Théoréme d'incomplétude, bref résumé

Notes complémentaires (5)

Les conventions de notation sont les mêmes que dans les notes précédentes On continue la numérotation des sections et des propositions en suivant celle des notes n°4

13 Théorème d'incomplétude

13.1 Préliminaires

On rappelle que $\mathcal{L}_0$ est le langage de l'arithmétique. Pour les défintions de $\mathcal{P}_0, AP$, voir le cours.

13.1.1 Diagonalisation

Argument de diagonalisation: Soit E un ensemble, $P \subset E \times E$. Pour $e \in E$, $P_e = \{x \in E; (e,x) \in P\}$. Si $Q = \{x \in E; (x,x) \notin P\}$, alors $Q \neq P_e$ pour tout $e \in E$. (En effet, si on suppose que $Q = P_e$, alors $e \in Q$ ssi $e \notin Q$.)

C'est cet argument que l'on applique par exemple dans la preuve classique que $\mathcal{P}(X)$ est toujours de cardinalité strictement supérieure à celle de X. C'est aussi celui qui sert pour montrer qu'il existe un récursivement énumérable non récursif (voir section 13.2) et le théorème d'incomplétude.

13.1.2 Représentabilité

Définition:1. Une application totale $f : \mathbb{N}^k \mapsto \mathbb{N}$ est **représentable** si il existe une formule $\phi(w, v_1, \ldots, v_k)$ de $\mathcal{L}_0$ telle que, pour tout $(n_1, \ldots, n_k) \in \mathbb{N}^k$,

$$\mathcal{P}_0 \vdash \forall w(\phi(w, \underline{n}_1, \ldots, \underline{n}_k) \leftrightarrow w = \underline{m})$$

où $m = f(n_1, \ldots, n_k)$.

2. Soit $E \subset \mathbb{N}^k$, E est **fortement représentable** dans $\mathcal{P}_0$ si il existe une formule $\phi(v_1, \ldots, v_k)$ de $\mathcal{L}_0$ telle que, pour tout $(n_1, \ldots, n_k) \in \mathbb{N}^k$,

- si $(n_1, \ldots, n_k) \in E$, alors $\mathcal{P}_0 \vdash \phi(\underline{n}_1, \ldots, \underline{n}_k)$,
- $(n_1, \ldots, n_k) \notin E$, alors $\mathcal{P}_0 \vdash \neg\phi(\underline{n}_1, \ldots, \underline{n}_k)$.

Lemme 13.1 *Un ensemble $E \subset \mathbb{N}^k$ est fortement représentable ssi sa fonction caractéristique, χ_E est représentable.*

Remarques: - Attention, la définition de fortement représentable est plus forte que de dire $(n_1, \ldots, n_k) \in E$ ssi $\mathcal{P}_0 \vdash \phi(\underline{n_1}, \ldots, \underline{n_k})$!
- Un ensemble E fortement représentable dans $\mathcal{P}_0$ est $\mathcal{L}_0$-définissable dans $\mathbb{N}$ mais la réciproque n'est pas vraie.
- Une application de $\mathbb{N}^k$ dans $\mathbb{N}$ qui est représentable est définissable dans $\mathbb{N}$ par la formule $\phi(w, v_1, \ldots, v_k)$, qui donne son graphe. Mais la formule $\phi(w, v_1, \ldots, v_k)$ ne définit pas forcément un graphe de fonction dans tout modèle de $\mathcal{P}_0$!

Définition:1. L'ensemble des **formules** Σ_0^1 de l'arithmétique est le plus petit sous-ensemble de formules qui contient les formules sans quantificateurs et qui est clos par $\wedge$, $\vee$, par $\exists$ et par quantification universelle bornée, c'est-à-dire que si $\phi(v_0, v_1, \ldots, v_n, w)$ est une formule Σ_0^1, alors la formule

$$\forall w\, (w < v_0 \rightarrow \phi(v_0, v_1, \ldots, v_n, w))$$

est aussi une formule Σ_0^1.

Proposition 13.2 *Soit σ un énoncé Σ_0^1, alors, si $\mathbb{N} \models \sigma$, $AP \vdash \sigma$.*

13.2 Récursivité et définissabilité

13.2.1 Fonctions et ensembles récursifs

On considère F_k l'ensemble de toutes les fonctions partielles de domaine inclus dans $\mathbb{N}^k$ et à valeurs dans $\mathbb{N}$.
Définition: L'ensemble des **fonctions récursives partielles** est le plus petit sous-ensemble de $F = \bigcup_{k \geq 0} F_k$ qui contient les fonctions constantes, les projections, la fonction successeur, et est clos par composition, récursion et minimisation.

Sont récursives: l'identité, l'addition, la multiplication, l'exponentiation ($(x, y) \mapsto x^y$), le codage des suites finies d'entiers.
Remarque: il n'y a qu'un nombre dénombrable de fonctions récursives.

Soient deux fonctions récursives partielles f et g de $\mathbb{N}^k$ dans $\mathbb{N}$, on dit que f et g sont égales si pour tout $x \in \mathbb{N}^k$, x est dans le domaine de f ssi x est dans le domaine de g, et dans ce cas, $f(x) = g(x)$.
Définitions: 1. Un ensemble $A \subseteq \mathbb{N}^k$ est **récursif** si sa fonction caractéristique est récursive.

2. Un ensemble $A \subseteq \mathbb{N}^k$ est **récursivement énumérable** si A est le domaine d'une fonction récursive partielle.

Les ensembles finis, la diagonale, sont récursifs.

Proposition 13.3 (Propriétés) *(i) Si A est récursif, A est récursivement énumérable.*

(ii) L'ensemble des sous-ensembles récursifs de $\mathbb{N}^k$ est clos par réunion finie, intersection finie et complémentaire.

(iii) L'ensemble des sous-ensembles récursivement énumérables de $\mathbb{N}^k$ est clos par réunion finie, intersection finie et projection.

(iv) A est récursif si et seulement si A et $\mathbb{N}^k \setminus A$ sont tous les deux récursivement énumérables.

Proposition 13.4 (Existence d'une fonction récursive universelle). *Il existe une fonction récursive partielle $\phi : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$ telle que, pour chaque fonction récursive partielle f de $\mathbb{N}$ dans $\mathbb{N}$, il existe $i \in \mathbb{N}$ tel que pour chaque $x \in \mathbb{N}$, $f(x) = \phi((i, x)$.*

Corollaire 13.5 *Il existe un ensemble récursivement énumérable non récursif.*

Démonstration : Soit $W \subset \mathbb{N} \times \mathbb{N}$ défini de la façon suivante: n – $(n, m) \in W$ ssi $\phi(n, m)$ est définie, c'est-à-dire, si m appartient au domaine de la fonction récursive partielle f_n égale à $\phi(n, -)$.

Si $W_n = \{m \in \mathbb{N}; (n, m) \in W\}$, on voit que si $E \subset \mathbb{N}$, E est récursivement énumérable ssi il existe n tel que $E = W_n$.

On considère $Q \subset \mathbb{N}$, défini par $Q = \{n \in \mathbb{N}; (n, n) \in W\}$. Alors Q est un ensemble récursivement énumérable car c'est le domaine de la fonction récursive partielle $\phi(x, x)$. Soit $\widetilde{Q}$ le complémentaire de Q, $\widetilde{Q} = \{n \in \mathbb{N}; (n, n) \notin W\}$. L'argument de diagonalisation (13.1.1) montre que $\widetilde{Q}$ n'est pas récursivement énumérable, donc par 13.3, Q n'est pas récursif. $\square$

13.2.2 Calculabilité et représentabilité

Quatre notions différentes pour une fonction:
– calculable, notion "intuitive"
– calculable par une machine de Türing , definition formelle d'une machine "théorique"
– récursive
– représentable (notion de type "théorie des modèles").

La thèse de Church dit que calculable = calculable par une machine de Turing.

Les autres équivalences, qui portent elles, sur des notions bien définies sont des théorèmes.

Théorème 13.6 *1. Fonction récursive partielle = fonction calculable par une machine de Turing*

2. Si f est une fonction totale de $\mathbb{N}^k$ dans $\mathbb{N}$, f est représentable dans $\mathcal{P}_0$ si et seulement si f est récursive.

Et le corollaire qui va nous servir directement pour la suite:

Corollaire 13.7 *Si $E \subset \mathbb{N}^k$ est récursif, alors E est fortement représentable dans $\mathcal{P}_0$.*

Remarque: En fait, si f est une fonction totale récursive de $\mathbb{N}^k$ dans $\mathbb{N}$, alors f est représentable par une formule Σ^1_0. Cette analyse plus fine est nécessaire pour démontrer le deuxième théorème d'incomplétude.

13.3 Codages et Décidabilité

Soit $\mathcal{L}$ un langage fini $\mathcal{L} \supseteq \mathcal{L}_0$ et $\mathcal{L}*$ l'ensemble de tous les mots de $\mathcal{L}$. A chaque mot de $\mathcal{L}$, s, on associe injectivement un entier, le **code** (de Gödel) de s, noté $[s]$, de façon que les opérations habituelle que l'on opère sur les formules soient données par des fonctions récursives, On veut également que les ensembles suivants soient récursifs:

– $A_1 = \{n \in \mathbb{N}; n = [s]$ pour $s \in \mathcal{L}*\}$
–$A_2 = \{n \in \mathbb{N}; n = [t]$ pour t terme de $\mathcal{L}\}$
–$A_3 = \{n \in \mathbb{N}; n = [\phi]$ pour ϕ formule de $\mathcal{L}\}$
–$A_4 = \{n \in \mathbb{N}; n = [\phi(v_0)]$ pour $\phi(v_0)$ formule à variable libre v_0 de $\mathcal{L}\}$
–$A_5 = \{n \in \mathbb{N}; n = [\sigma]$ pour σ énoncé de $\mathcal{L}\}$.

On utilisera par exemple: il y a une fonction récursive $f_\neg$ telle que $f_\neg[\sigma] = [\neg\sigma]$ et il y a une fonction récursive g_{sub} telle que, si $n \in A_4$, donc $n = [\phi(v_0)]$, $g_{sub}(n, m) = p$ où p est le code de l'énoncé $\phi(\underline{n})$.

Exemple de codage classique: On associe à chaque symbole de $\mathcal{L}$ et à chaque symbole logique (connecteurs, quantificateurs, parenthèses, variables) un entier, noté, pour un symbole s, $c(s)$. Ensuite, si on a un mot $m = s_1 \dots s_n$, on pose $[m] = \Pi_{1 \leq j \leq n} {p_j}^{c(s_j)}$, où p_j est le j^{ieme} nombre premier.(On trouve un codage un peu différent fait en détail dans le livre Cori-Lascar).

Définition: Soit T une théorie de $\mathcal{L}$.

1. La théorie T est **récursive** si l'ensemble $[T] = \{[\sigma]; \sigma \in T\}$ est récursif.
2. La théorie T est **décidable** si $[ConsT] = \{[\sigma] : T \vdash \sigma\}$ est récursif.

Toute théorie finie est récursive, en particulier $\mathcal{P}_0$ est récursive. La théorie AP est récursive.
On a également un codage des démonstrations formelles et on peut vérifier que si T est récursive, alors l'ensemble suivant est récursif:

$$Dem(T) = \{(n, m) \in \mathbb{N}^2; n = [\sigma] \text{ et } m \text{ est le code d'une démonstration de } T \vdash \sigma\}.$$

Proposition 13.8 *Si T est récursive, alors $[ConsT]$ est récursivement énumérable.*
Si T est récursive et complète, alors T est décidable.

Démonstration : $n \in [ConsT]$ si et seulement si il existe m tel que $(n, m) \in Dem(T)$ et c'est donc la projection d'un ensemble récursif.

Si T est complète, alors le complémentaire de $[ConsT]$ est l'ensemble des n pour lesquels il existe m tel que $(f_\neg(n), m) \in Dem(T)$; [Cons T] et son complémentaire sont donc tous les deux récursivement énumérables, ils sont donc récursifs. □

13.4 Les théorèmes d'incomplétude

13.4.1 Le premier théorème d'incomplétude

Proposition 13.9 (Théorème d'indécidabilité) *Soit $\mathcal{L}$ un langage fini contenant $\mathcal{L}_0$, et T un ensemble consistant d'énoncés de $\mathcal{L}$ contenant $\mathcal{P}_0$. Alors T n'est pas décidable.*

Démonstration : On considère

$$D(T) = \{(m, n) \in \mathbb{N}^2; m \text{ est le code d'une formule } \phi(v_0) \text{ de } \mathcal{L} \text{ et } T \vdash \phi(\underline{n})\}$$

et $D(T)_m = \{n \in \mathbb{N}; (m, n) \in D(T)\}$. (On remarque que si T est décidable, alors $D(T)$ est récursif: $(m, n) \in D(T)$ ssi $m \in A_4$ et $g_{sub}(m, n) \in [ConsT]$.)

a) Si $E \subseteq \mathbb{N}$ est un ensemble récursif, alors il est représentable dans $\mathcal{P}_0$ par 13.7. Il existe donc une formule $\phi(v_0)$ de $\mathcal{L}_0$ telle que:

– si $n \in E$, alors $P_0 \vdash \phi(\underline{n})$, donc $T \vdash \phi(\underline{n})$

– si $n \notin E$, alors $P_0 \vdash \neg\phi(\underline{n})$, T étant consistante, donc $T \not\vdash \phi(\underline{n})$.

Donc en fait, $n \in E$ si et seulement si $T \vdash \phi(\underline{n})$.

Donc si m est le code de la formule $\phi(\underline{n})$

$$E = \{n \in \mathbb{N}; T \vdash \phi(\underline{n})\} = \{n \in \mathbb{N}; (m, n) \in D(T)\} = D(T)_m.$$

b) Soit maintenant $Q = \{n \in \mathbb{N}; (n, n) \notin D(T)\}$. L'argument diagonal classique (13.1.1) entraîne que $Q \neq D(T)_m$ pour tout m. Donc par a), Q n'est pas un ensemble récursif.

c) Si T est décidable, c'est-à-dirs si $[Cons(T)]$ est récursif, alors Q est récursif aussi: en effet $n \in Q$ ssi ($n \in A_4$ et $g_{sub}(n, n) \in \mathbb{N} \setminus [Cons(T)]$). □

Maintenant, on obtient directement, en utilisant la Proposition 13.8:

Corollaire 13.10 (Premier théorème d'incomplétude) *Si T est une théorie consistante et récursive qui étend $\mathcal{P}_0$, alors T n'est pas complète.*

Corollaire 13.11 (Indécidabilité du calcul des prédicats) *Soit $\mathcal{L} \supseteq \mathcal{L}_0$, $\mathcal{L}$ fini. Alors l'ensemble des énoncés valides de $\mathcal{L}$ est indécidable.*

Démonstration : Soit $Val(\mathcal{L}) = \{\phi \in \mathcal{L}; \vdash \phi\}$.

La théorie $\mathcal{P}_0$ est composée d'un nombre fini d'énoncés, en prenant leur conjonction, on peut donc la remplacer par un seul énoncé, θ_0. Alors, pour tout énoncé σ de $\mathcal{L}_0$,

$$\mathcal{P}_0 \vdash \sigma \text{ ssi } \vdash (\theta_0 \rightarrow \sigma) \text{ ssi } (\theta_0 \rightarrow \sigma) \in Val(\mathcal{L}).$$

Si $Val(\mathcal{L})$ était décidable, $\mathcal{P}_0$ le serait aussi. □

13.4.2 Le deuxième théorème d'incomplétude

Le premier théorème d'incomplétude nous dit qu'il existe des énoncés σ du langage de l'arithmétique tels que $AP \not\vdash \sigma$ et $AP \not\vdash \neg\sigma$. Le deuxième théorème d'incomplétude exhibe un tel σ, l'énoncé $Con(AP)$, dont l'interprétation est “ AP est une théorie consistante” . On travaille maintenant avec la théorie AP, c'est une théorie récursive , donc l'ensemble

$$Dem(AP) = \{(n, m) \in \mathbb{N}^2; n = [\sigma] \text{ et } m \text{ est le code d'une démonstration de } T \vdash \sigma\}$$

est récursif.
Cet ensemble est donc fortement représentable dans $\mathcal{P}_0$, donc aussi dans AP. Il existe donc une formule $pr(x,y)$ de $\mathcal{L}_0$ telle que pour tout $(n,m) \in \mathbb{N}^2$,

– si $(n,m) \in Dem(AP)$, alors $AP \vdash pr(\underline{n}, \underline{m})$,
– si $(n,m) \notin Dem(AP)$, alors $AP \vdash \neg pr(\underline{n}, \underline{m})$.

Si σ est un énoncé de $\mathcal{L}_0$, alors

$$(*) \quad AP \vdash \sigma \text{ ssi } \mathbb{N} \models \exists y\, pr([\sigma], y) \text{ ssi } AP \vdash \exists y\, pr(\underline{[\sigma]}, y).$$

En effet, si $\mathbb{N} \models \exists y\, pr([\sigma], y)$, alors il existe m tel que $([\sigma], m) \in Dem(AP)$, donc par forte représentation, on a $AP \vdash pr(\underline{[(\sigma]}, \underline{m})$, donc $AP \vdash \exists y\, pr(\underline{[\sigma]}, y)$. Réciproquement, si $AP \vdash \exists y\, pr(\underline{[\sigma]}, y)$, alors $\mathbb{N} \models \exists y\, pr(\overline{[\sigma]}, y$.

Considérons maintenant la formule suivante,

$$(**) \quad \psi(w) = (w \in A_5 \wedge (\exists v_1\, pr(w, v) \ \wedge \exists v_2\, pr(g_\neg(w), v_2)).$$

On voit que si $\mathbb{N} \models \psi(r)$, et si $r = [\sigma]$, alors $AP \vdash \sigma$ et $AP \vdash \neg\sigma$. On appelle donc $Con(AP)$ (Consistance de AP) l'énoncé $\neg(\exists w\, \psi(w))$. Et on a donc $\mathbb{N} \models Con(AP)$, et $AP \not\vdash \neg(Con(AP)$.

Proposition 13.12 (Deuxième théorème d'incomplétude)

$$AP \not\vdash Con(AP).$$

Pour démontrer ce résultat nous allons admettre la proposition suivante, dans laquelle se trouve concentrées les difficultés techniques:

Proposition 13.13 *On peut choisir une formule $pr(v,w)$ qui représente l'ensemble $Dem(AP)$, qui est Σ^1_0, et telle que, pour tout énoncé Σ^1_0, σ,*

$$(***) \quad AP \vdash (\sigma \ \rightarrow \ \exists v\, pr(\underline{[\sigma]}, v)).$$

On remarque que $(***)$ n'est pas conséquence de $(*)$.
La propriété demandée est vraie dans $\mathbb{N}$ avec n'importe quel choix pour la formule $pr(v,w)$: En effet soit σ un énoncé Σ^1_0. Alors, si $\mathbb{N} \models \sigma$, $AP \vdash \sigma$ (Proposition 13.2) et donc, $\mathbb{N} \vdash \exists v\, pr(\underline{[\sigma]}, v)$, donc on a bien $\mathbb{N} \models (\sigma \ \rightarrow \ \exists v\, pr(\underline{[\sigma]}, v))$. Mais dans $(***)$, on demande que cela soit vrai pour *tout* modèle de AP.

Avec la Proposition, nous pouvons terminer la démonstration:
Soit $\theta(v_0)$ la formule suivante : $\exists v\, pr(g_{sub}(v_0, v_0), v)$.
Donc si $n = [\phi(v_0)]$ on a $AP \vdash \theta(\underline{n})$ ssi $AP \vdash \phi(\underline{n})$.
Maintenant considérons $m = [\neg\theta(v_0)]$. Alors

$$AP \vdash \theta(\underline{m}) \text{ ssi } AP \vdash \neg\theta(\underline{m}).$$

Donc, on a:

$$(****) \quad AP \not\vdash \theta(\underline{m}) \text{ et } AP \not\vdash \neg\theta(\underline{m}).$$

Soit $\alpha = \underline{[\theta(\underline{m})]}$. L'énoncé $\theta(\underline{m})$ est Σ^1_0, donc par la proposition,

$$AP \vdash \theta(\underline{m}) \rightarrow \exists v_1\, pr(\alpha, v_1),$$

et, par la définition de $\theta(v_0)$,

$$AP \vdash \theta(\underline{m}) \rightarrow \exists v_2\, pr(g_\neg(\alpha), v_2).$$

Donc par $(**)$,

$$AP \vdash \theta(\underline{m}) \rightarrow \exists w\, \psi(w)$$

c'est-à-dire

$$AP \vdash \theta(\underline{m}) \rightarrow \neg Con(AP).$$

D'où, $AP \vdash (Con(AP) \rightarrow \neg\theta(\underline{m}))$, ce qui entraine bien par $(****)$ que

$$AP \nvdash Con(AP).$$