TD7 - Théorème de Church

Définition 1 ($\mathbb{N}$-modèle). Soit $\mathcal{L}$ un langage et N, $Null$, $Succ$, $Plus$, $Mult$ et Eq des propositions de ce langage.

Un modèle $\mathcal{M}$ de $\mathcal{L}$ est un $\mathbb{N}$-*modèle* si :

$$\begin{gathered}\{\, a \in \mathcal{M} \mid [\![N]\!]_{x=a} = 1 \} = \mathbb{N} \\ \{\, a \in \mathbb{N} \mid [\![Null]\!]_{x=a} = 1 \} = \{0\} \\ \left\{ (a,b) \in \mathbb{N}^2 \,\middle|\, [\![Succ]\!]_{x=a,y=b} = 1 \right\} = \left\{ (a,b) \in \mathbb{N}^2 \,\middle|\, b = a+1 \right\} \\ \left\{ (a,b,c) \in \mathbb{N}^3 \,\middle|\, [\![Plus]\!]_{x=a,y=b,z=c} = 1 \right\} = \left\{ (a,b,c) \in \mathbb{N}^3 \,\middle|\, c = a+b \right\} \\ \left\{ (a,b,c) \in \mathbb{N}^3 \,\middle|\, [\![Mult]\!]_{x=a,y=b,z=c} = 1 \right\} = \left\{ (a,b,c) \in \mathbb{N}^3 \,\middle|\, c = a \times b \right\} \\ \left\{ (a,b) \in \mathbb{N}^2 \,\middle|\, [\![Eq]\!]_{x=a,y=b} = 1 \right\} = \left\{ (a,b) \in \mathbb{N}^2 \,\middle|\, b = a \right\}\end{gathered}$$

Définition 2 (Proposition N_q). Dans le langage $\mathcal{L}$ de la définition précédente, on définit pour tout entier n une proposition N_n par :

$$\begin{aligned} N_0 &= Null[x] \\ N_{n+1} &= \exists y.(N_n[y] \wedge Succ[y,x]) \end{aligned}$$

Exercice 1. La démonstration du cours

Soit $\mathcal{L}$ un langage, N, $Null$, $Succ$, $Plus$, $Mult$ et Eq des propositions de $\mathcal{L}$ et $\mathcal{T}$ une théorie dans ce langage qui démontre au moins les axiomes de la théorie $\mathcal{T}_0$ et qui a un $\mathbb{N}$-modèle $\mathcal{M}$.

Question 1. Montrer que si f est un programme et A la proposition représentant f, les trois propositions suivantes sont équivalentes :

- f prend la valeur q en $p_1, \dots, p_n$,
- la proposition $\forall x_1. \dots \forall x_n. \forall y. ((N_{p_1}[x_1] \wedge \dots \wedge N_{p_n}[x_n] \wedge N_q[y]) \Rightarrow A[x_1, \dots, x_n, y])$ est démontrable dans $\mathcal{T}$,
- cette proposition est valide dans le modèle $\mathcal{M}$.

Exercice 2. Un exemple de proposition indéterminée

Soit $\mathcal{L}$ un langage, N, $Null$, $Succ$, $Plus$, $Mult$ et Eq des propositions de ce langage et $\mathcal{T}$ une théorie dont l'ensemble des axiomes est décidable et qui a un $\mathbb{N}$-modèle $\mathcal{M}$. Soit $\mathcal{T}'$ la théorie $\mathcal{T} \cup \mathcal{T}_0$.

Soit f la fonction calculable telle que $f(n,p,q) = 1$ si $n = \lceil \pi \rceil$, $p = \lceil A \rceil$ et π est une démostration dans $\mathcal{T}'$ de la proposition $\forall w.(N_q[w] \Rightarrow A)$ et $f(n,p,q) = 0$ sinon.

Soit F la proposition représentant un programme exprimant cette fonction.

Soit T la proposition

$$\forall x.\forall y.\left((N[x] \wedge N_1[y]) \Rightarrow \neg F[x,w,w,y]\right),$$

$m = \lceil T \rceil$ et G la proposition close

$$\forall w.(N_m[w] \Rightarrow T)$$

Question 2. Montrer que si G est démontrable dans $\mathcal{T}'$ alors

1. $[\![G]\!] = 1$,
2. pour tout entier n, $[\![F]\!]_{x_1=n,x_2=m,x_3=m,y=1} = 0$,
3. pour tout entier n, $f(n,m,m) = 0$,
4. la proposition $\forall w.(N_m[w] \Rightarrow T)$ n'est pas démontrable dans $\mathcal{T}'$,
5. la proposition G n'est pas démontrable dans $\mathcal{T}'$.

En déduire que G n'est pas démontrable dans $\mathcal{T}$.

Question 3. Montrer que si $\neg G$ est démontrable dans $\mathcal{T}'$ alors

1. $[\![\neg G]\!] = 1$,
2. il existe un entier n tel que, $[\![F]\!]_{x_1=n,x_2=m,x_3=m,y=1} = 1$,
3. il existe un entier n tel que, $f(n,m,m) = 1$,
4. la proposition $\forall w.(N_m[w] \Rightarrow T)$ est démontrable dans $\mathcal{T}'$,
5. la proposition G est démontrable dans $\mathcal{T}'$,
6. la théorie $\mathcal{T}'$ est contradictoire.

En déduire que $\neg G$ n'est pas démontrable dans $\mathcal{T}$.

Exercice 3. Une proposition vraie pour tout entier mais indémontrable

Dans cet exercice, on admettra le théorème de Matiyasevich, c'est-à-dire que l'ensemble des propositions démontrables dans l'arithmétique de la forme $\exists x_1 \ldots \exists x_m.(t = u)$ est indécidable.

Question 4. Montrer qu'il existe une proposition close A de la forme $\exists x_1 \ldots . \exists x_m.(t = u)$ telle que ni A ni $\neg A$ ne soient démontrables dans l'arithmétique.

Question 5. Montrer que la proposition $\forall x_1 \ldots \forall x_m.\neg(t = u)$ n'est pas démontrable.

Question 6. Montrer que si a est un terme clos de l'arithmétique, alors il existe un entier n tel que la proposition $a = \underline{n}$ soit démontrable.

Question 7. Montrer que si n et p sont deux entiers, alors ou bien la proposition $\underline{n} = \underline{p}$ est démontrable ou bien la proposition $\neg(\underline{n} = \underline{p})$ est démontrable.

Question 8. Montrer que si a et b sont deux termes clos de l'arthmétique, alors la proposition $a = b$ est démontrable ou la proposition $\neg(a = b)$ est démontrable.

Question 9. Soit une équation $t = u$ dont les variables sont parmi $x_1, \ldots, x_m$ et $p_1, \ldots, p_m$ des entiers tels que la proposition $(t = u)[\underline{p_1}/x_1, \ldots, \underline{p_m}/x_m]$ soit démontrable. Montrer que la proposition $\exists x_1 \ldots \exists x_m.(t = u)$ est démontrable. Montrer que si la proposition $\exists x_1 \ldots \exists x_m.(t = u)$ n'est pas démontrable, alors pour tout $p_1, \ldots, p_m$, la proposition $(t = u)[\underline{p_1}/x_1, \ldots, \underline{p_m}/x_m]$ n'est pas démontrable.

Question 10. Montrer que si la proposition $\exists x_1 \ldots \exists x_m.(t = u)$ n'est pas démontrable, alors pour tout $p_1, \ldots, p_m$, la proposition $\neg(t = u)[\underline{p_1}/x_1, \ldots, \underline{p_m}/x_m]$ est démontrable.

Question 11. Montrer qu'il existe une proposition A de la forme $\neg(t = u)$ dont les variables sont parmi $x_1, \ldots, x_m$ et telle que

- pour tout $p_1, \ldots, p_m$ la proposition $A[\underline{p_1}, \ldots, \underline{p_m}]$ est démontrable
- la proposition $\forall x_1 \ldots \forall x_m.A$ n'est pas démontrable.

Exercice 4. Théorème de Church

Le théorème de Church dit que si un langage contient au moins un symbole de prédicat binaire, alors l'ensemble des propositions closes démontrables dans la théorie vide de ce langage est indécidable.

Question 12. Construire un $\mathbb{N}$-modèle $\mathcal{M}$ de ce langage tel que $M = \mathbb{N} \cup (\mathbb{N} \times \mathbb{N})$ et $R^{\mathcal{M}} = \{ (a, (a, b)) | \, a \in \mathbb{N}, b \in \mathbb{N}\} \cup \{ ((a, b), b) | \, a \in \mathbb{N}, b \in \mathbb{N}\} \cup \{ ((a, b), (a + b, a \times b)) | \, a \in \mathbb{N}, b \in \mathbb{N}\}$.