# 5
# *Le théorème de Church*

Une partie importante de l'activité mathématique consiste à concevoir des algorithmes qui permettent de résoudre des problèmes, par exemple calculer le plus grand diviseur commun de deux entiers, la solution d'un système linéaire ou la primitive d'une fonction polynomiale, sans construire de démonstration. Jusqu'à quel point est-il possible de remplacer la recherche d'une démonstration par l'exécution d'un algorithme ? Un ensemble de résultats, tant négatifs que positifs, précise ce qu'il est possible de faire.

Ce chapitre est consacré à deux résultats, l'un négatif et l'autre positif, qui montrent que l'ensemble des propositions démontrables dans la logique des prédicats n'est pas décidable, mais qu'il est semi-décidable.

Comme tous les arbres, les propositions peuvent se numéroter. Ces résultats montrent donc, plus précisément, que l'ensemble des numéros des propositions démontrables dans la logique des prédicats n'est pas décidable, mais qu'il est semi-décidable.

## 5.1 La notion de réduction

Commençons par montrer que l'ensemble des propositions démontrables dans la logique des prédicats n'est pas décidable. L'idée de la démonstration peut se formuler en une phrase : le fait qu'un programme $f$ termine peut s'exprimer par la proposition « Le programme $f$ termine » et, puisqu'il est impossible de décider la terminaison des programmes, il est impossible de décider

la démontrabilité des propositions de ce type et donc de la démontrabilité des propositions en général.

Qu'est-ce que la proposition : « Le programme $f$ termine » ? Répondre à cette question consiste à associer à chaque programme $f$, une proposition qui est démontrable si et seulement si le programme $f$ termine. Comme nous allons le voir, la fonction $T$ qui, au programme $f$, associe la proposition « Le programme $f$ termine » est calculable. De ce fait, s'il existait une fonction calculable $F$ pour décider si une proposition est démontrable ou non, la fonction $F \circ T$ serait calculable en contradiction avec le théorème d'indécidabilité du problème de l'arrêt.

On voit apparaître ici une méthode assez générale pour montrer qu'un problème est indécidable : construire un algorithme qui permet de réduire, au problème en question, un problème déjà démontré indécidable, dans cet exemple, le problème de l'arrêt. Cela peut se formuler de manière abstraite comme le fait que, l'ensemble des fonctions calculables étant clos par composition, si $T$ est calculable et $F \circ T$ ne l'est pas, alors $F$ ne l'est pas non plus.

## 5.2 La représentation des programmes

On commence par associer à chaque programme $f$ d'arité $n$ une proposition $A$ de l'arithmétique dont les variables libres sont parmi $x_1, \ldots, x_n, y$ qui *représente* le programme $f$. Cela signifie que la proposition $(\underline{p_1}/x_1, \ldots, \underline{p_n}/x_n, \underline{q}/y)A$, où $\underline{p}$ est le terme $S^p(0)$, est démontrable si et seulement si $f$ prend la valeur $q$ en $p_1, \ldots, p_n$. Pour simplifier les notations, on écrit $A[t_1, \ldots, t_n, u]$ la proposition $(t_1/x_1, \ldots, t_n/x_n, u/y)A$.

Si $f = \pi_i^n$, on peut poser $A = (y = x_i)$. Si $f = Z^n$, $A = (y = 0)$. Si $f = Succ$, $A = (y = S(x_1))$. Si $f = +$, $A = (y = x_1 + x_2)$. Si $f = \times$, $A = (y = x_1 \times x_2)$. Si $f = \chi_{\leq}$, $A = (x_1 \leq x_2 \wedge y = 1) \vee (x_2 < x_1 \wedge y = 0)$ où la proposition $x \leq y$ est une abréviation pour $\exists z\ (z + x = y)$ et la proposition $x < y$ pour $S(x) \leq y$.

Si $f = \circ_m^n(h, g_1, \ldots, g_m)$, on commence par construire des propositions $B_1$, $\ldots$, $B_m$ et $C$ représentant les programmes $g_1$, $\ldots$, $g_m$ et $h$ et on pose

$$A = \exists w_1 \ldots \exists w_m\ (B_1[x_1, \ldots, x_n, w_1] \wedge \ldots \wedge B_m[x_1, \ldots, x_n, w_m] \wedge C[w_1, \ldots, w_m, y])$$

Enfin, si $f = \mu^n(g)$, on commence par construire une proposition $B$ représentant le programme $g$ et on pose

$$A = (\forall z\ (z < y \Rightarrow \exists w\ (B[x_1, \ldots, x_n, z, S(w)]))) \wedge B[x_1, \ldots, x_n, y, 0]$$

Nous pourrions alors démontrer que $f$ prend la valeur $q$ en $p_1, \ldots, p_n$ si et seulement si la proposition $A[\underline{p_1}, \ldots, \underline{p_n}, \underline{q}]$ est démontrable dans l'arithmétique, et conclure que la démontrabilité dans l'arithmétique est indécidable.

Cependant, avant d'entreprendre cette démonstration, nous allons étendre quelque peu la définition ci-avant. Celle-ci suppose, en effet, que le langage contient des symboles 0, $S$, $+$, $\times$ et $=$ et également que l'univers du discours est limité aux entiers. Ces deux hypothèses sont vérifiées dans le cas de l'arithmétique, mais elles seront des obstacles, quand nous voudrons généraliser ce résultat à d'autres théories. Par exemple, nous avons vu que dans le langage de la théorie des ensembles, il n'y a pas de symbole $S$ pour le successeur, mais il y a une proposition, contentant deux variables libres $x$ et $y$, qui exprime le fait que $y$ est le successeur de $x$

$$\forall z\ (z \in y \Leftrightarrow (z \in x \vee z = x))$$

Nous considérons donc un langage quelconque, dans lequel il est possible de construire des propositions $N$, *Null*, *Succ*, *Plus*, *Mult* et *Eq*. Nous écrivons $N[t]$ la proposition $(t/x)N$, $Succ[t,u]$ la proposition $(t/x,u/y)Succ$, ... Par exemple, dans l'arithmétique, $N$ est la proposition $\top$, *Null* la proposition $x = 0$, *Succ* la proposition $y = S(x)$, *Plus* la proposition $z = x + y$, *Mult* la proposition $z = x \times y$ et *Eq* la proposition $x = y$. En théorie des ensembles, la proposition $N$ est celle construite dans l'exercice 1.17, la proposition *Succ* est la proposition $\forall z\ (z \in y \Leftrightarrow (z \in x \vee z = x))$, ...

La proposition *Inf*, *relation d'ordre*, se définit comme $\exists z\ (N[z] \wedge Plus[z,x,y])$ et *InfS*, *relation d'ordre strict*, comme $\exists x'\ (N[x'] \wedge Succ[x,x'] \wedge Inf[x',y])$.

Dans ce langage, nous associons une proposition à chaque programme.

## Définition 5.1 (Proposition représentant un programme)

Soit $f$ un programme d'arité $n$, la proposition $A$ *représentant* $f$ est définie par récurrence sur la construction de $f$.

- Si $f = \pi_i^n$, on pose $A = Eq[x_i, y]$.
- Si $f = Z^n$, on pose $A = Null[y]$.
- Si $f = Succ$, on pose $A = Succ[x_1, y]$.
- Si $f = +$, on pose $A = Plus[x_1, x_2, y]$.
- Si $f = \times$, on pose $A = Mult[x_1, x_2, y]$.
- Si $f = \chi_{\leq}$, on pose $A = (Inf[x_1, x_2] \wedge \exists z\ (Null[z] \wedge Succ[z, y])) \vee (InfS[x_2, x_1] \wedge Null[y])$.
- Si $f = \circ_m^n(h, g_1, \ldots, g_m)$, alors soient $B_1$, ..., $B_m$ et $C$ les propositions représentant les programmes $g_1$, ..., $g_m$ et $h$, on pose

  $$A = \exists w_1 \ldots \exists w_m\ (N[w_1] \wedge \ldots \wedge N[w_m] \wedge B_1[x_1, \ldots, x_n, w_1] \wedge \ldots \wedge B_m[x_1, \ldots, x_n, w_m] \wedge C[w_1, \ldots, w_m, y]).$$
- Si $f = \mu^n(g)$, alors soit $B$ la proposition représentant le programme $g$, on pose

$$A = (\forall z\ (N[z] \wedge \mathit{InfS}[z,y] \Rightarrow \exists w \exists w'\ (N[w'] \wedge \mathit{Succ}[w',w] \wedge B[x_1,\ldots,x_n,z,w]))) \wedge (\forall w\ (\mathit{Null}[w] \Rightarrow B[x_1,\ldots,x_n,y,w])).$$

Nous voulons alors démontrer que $f$ prend la valeur $q$ en $p_1,\ldots,p_n$ si et seulement si la proposition $A$ relie les nombres $p_1,\ldots,p_n,q$. Cependant, nous ne pouvons plus exprimer cela simplement en substituant aux variables des termes de la forme $S^p(0)$ dans la proposition $A$, car nous ne disposons plus nécessairement des symboles 0 et $S$. Nous devons alors introduire, pour chaque entier, une proposition $N_n$ qui caractérise l'entier $n$, en posant $N_0 = \mathit{Null}[x]$ et $N_{n+1} = \exists y\ (N_n[y] \wedge \mathit{Succ}[y,x])$. Si une proposition $A$ contient potentiellement une variable libre $x$, nous pouvons exprimer le fait que la propriété exprimée par $A$ s'applique à l'entier $n$ par la proposition $\forall x\ (N_n[x] \Rightarrow A)$.

Nous pouvons alors démontrer que $f$ prend la valeur $q$ en $p_1,\ldots,p_n$ si et seulement si la proposition

$$\forall x_1 \ldots \forall x_n \forall y\ ((N_{p_1}[x_1] \wedge \ldots \wedge N_{p_n}[x_n] \wedge N_q[y]) \Rightarrow A[x_1,\ldots,x_n,y])$$

est démontrable. Naturellement, pour démontrer cette proposition, nous avons besoin de quelques propriétés des propositions *N*, *Null*, *Succ*, *Plus*, *Mult* et *Eq*. De façon surprenante, peu de propriétés suffisent. Ces propriétés sont rassemblées dans la théorie $\mathcal{T}_0$ suivante.

## Définition 5.2 (La théorie $\mathcal{T}_0$)

La théorie $\mathcal{T}_0$ est formée des axiomes suivants.
Prédicat *N* :

$$\forall x\ (\mathit{Null}[x] \Rightarrow N[x])$$

$$\forall x \forall y\ ((N[x] \wedge \mathit{Succ}[x,y]) \Rightarrow N[y])$$

Existence des entiers :

$$\exists x\ \mathit{Null}[x]$$

$$\forall x\ (N[x] \Rightarrow \exists y\ \mathit{Succ}[x,y])$$

Égalité :

$$\forall x\ \mathit{Eq}[x,x]$$

$$\forall x \forall y\ (\mathit{Null}[x] \Rightarrow (\mathit{Null}[y] \Leftrightarrow \mathit{Eq}[x,y]))$$

$$\forall x \forall y \forall x' \forall y'\ ((N[x] \wedge \mathit{Succ}[x,x'] \wedge \mathit{Eq}[x,y]) \Rightarrow (\mathit{Succ}[y,y'] \Leftrightarrow \mathit{Eq}[x',y']))$$

Injectivité du successeur :

$$\forall x \forall y \forall x' \forall y'\ (\mathit{Succ}[x,x'] \wedge \mathit{Succ}[y,y'] \wedge \mathit{Eq}[x',y']) \Rightarrow \mathit{Eq}[x,y])$$

Un successeur est non nul :

$$\forall x \forall x' \ (Succ[x, x'] \Rightarrow \neg Null[x'])$$

Tout entier est nul ou un successeur :

$$\forall x \ (N[x] \Rightarrow (Null[x] \vee \exists y \ (N[y] \wedge Succ[y, x])))$$

Addition :

$$\forall x \forall y \forall z \ ((Null[x] \wedge N[y]) \Rightarrow (Eq[y, z] \Leftrightarrow Plus[x, y, z]))$$

$$\forall x \forall y \forall z \forall x' \forall z' \ ((N[x] \wedge N[y] \wedge Plus[x, y, z] \wedge Succ[x, x']) \Rightarrow (Succ[z, z'] \Leftrightarrow Plus[x', y, z']))$$

$$\forall x \forall y \forall x' \forall y' \ ((N[x] \wedge N[y] \wedge Succ[x, x'] \wedge Succ[z, z'] \wedge Plus[x', y, z']) \Rightarrow Plus[x, y, z])$$

$$\forall x \forall y \forall y' \forall z' \ ((N[x] \wedge N[y] \wedge N[y'] \wedge Succ[y, y'] \wedge Plus[x, y', z']) \Rightarrow \exists z \ (Plus[x, y, z] \wedge Succ[z, z']))$$

Multiplication :

$$\forall x \forall y \forall z \ ((Null[x] \wedge N[y]) \Rightarrow (Null[z] \Leftrightarrow Mult[x, y, z]))$$

$$\forall x \forall y \forall z \forall x' \forall z' \ ((N[x] \wedge N[y] \wedge Mult[x, y, z] \wedge Succ[x, x']) \Rightarrow (Plus[y, z, z'] \Leftrightarrow Mult[x', y, z'])$$

## Proposition 5.1

Les propositions suivantes sont démontrables dans la théorie $\mathcal{T}_0$.

1. $\forall x \ (N_p[x] \Rightarrow N[x])$
2. $\exists x \ N_p[x]$
3. $\forall x \forall y \ (N_p[x] \Rightarrow (N_p[y] \Leftrightarrow Eq[x, y]))$
4. $\forall x \forall y \forall z \ ((N_p[x] \wedge N_q[y]) \Rightarrow (N_{p+q}[z] \Leftrightarrow Plus[x, y, z]))$
5. $\forall x \forall y \forall z \ ((N_p[x] \wedge N_q[y]) \Rightarrow (N_{p \times q}[z] \Leftrightarrow Mult[x, y, z]))$
6. $\forall x_1 \forall x_2 \ ((N_{p_1}[x_1] \wedge N_{p_2}[x_2]) \Rightarrow Inf[x_1, x_2])$, où $p_1 \leq p_2$
7. $\forall x_1 \forall x_2 \ ((N_{p_1}[x_1] \wedge N_{p_2}[x_2]) \Rightarrow InfS[x_1, x_2])$, où $p_1 < p_2$
8. $\forall x \forall y \forall y' \ ((N[x] \wedge Inf[x, y'] \wedge Succ[y, y']) \Rightarrow (Eq[x, y'] \vee Inf[x, y]))$
9. $\forall x \forall y \forall y' \ ((N[x] \wedge InfS[x, y'] \wedge Succ[y, y']) \Rightarrow (Eq[x, y] \vee InfS[x, y]))$
10. $\forall x \forall y \ ((N[x] \wedge InfS[x, y]) \Rightarrow \neg Null[y])$

*Démonstration.*

1. Par récurrence sur $p$, en utilisant les axiomes du prédicat $N$.
2. Par récurrence sur $p$, en utilisant les axiomes d'existence des entiers et (1.).
3. Par récurrence sur $p$, en utilisant les axiomes de l'égalité et (1.).

4. Par récurrence sur $p$, en utilisant les deux premiers axiomes de l'addition, (1.), (2.) et (3.).
5. Par récurrence sur $p$, en utilisant les axiomes de la multiplication, (1.), (2.) et (4.).
6. Comme $p_1 \leq p_2$, il existe un entier $q$ tel que $q + p_1 = p_2$. Des hypothèses $N_q[z]$, $N_{p_1}[x_1]$ et $N_{p_2}[x_2]$, on déduit, en utilisant (1.) et (4.), les propositions $N[z]$ et $Plus[z, x_1, x_2]$ et donc $Inf[x_1, x_2]$. On élimine ensuite l'hypothèse $N_q[z]$ avec (2.).
7. On a $p_1 < p_2$, et donc $p_1 + 1 \leq p_2$. Des hypothèses $N_{p_1}[x_1]$, $Succ[x_1, w]$ et $N_{p_2}[x_2]$, on déduit $N_{p_1+1}[w]$ puis, en utilisant (1.) et (6.), les propositions $N[w]$ et $Inf[w, x_2]$ et donc la proposition $InfS[x_1, x_2]$. On élimine ensuite l'hypothèse $Succ[x_1, w]$ en utilisant $\exists w\ Succ[x_1, w]$, qui se montre avec le second axiome d'existence des entiers.
8. La proposition $Inf[x, y']$ est $\exists z'\ (N[z'] \wedge Plus[z', x, y'])$. On utilise l'axiome *Tout entier est nul ou un successeur* pour distinguer le cas où $z'$ est nul et celui où c'est le successeur d'un entier $z$. Dans le premier cas, le premier axiome de l'addition donne $Eq[x, y']$. Dans le second, le troisième axiome de l'addition donne $Plus[z, x, y]$ et donc $Inf[x, y]$.
9. Conséquence de (8.) et de l'axiome *Injectivité du successeur*.
10. Conséquence du quatrième axiome de l'addition et de l'axiome *Un successeur est non nul*.

## Proposition 5.2

Soit $A$ une proposition. On écrit $A[t]$ la proposition $(t/x)A$. Si les propositions $\forall x\ (N_0[x] \Rightarrow A[x])$, $\forall x\ (N_1[x] \Rightarrow A[x])$, $\ldots$, $\forall x\ (N_{p-1}[x] \Rightarrow A[x])$ sont démontrables dans la théorie $\mathcal{T}_0$, alors c'est aussi le cas de la proposition $\forall x \forall y\ ((N[x] \wedge N_p[y] \wedge InfS[x, y]) \Rightarrow A[x])$.

*Démonstration.* Par récurrence sur $p$ en utilisant la proposition 5.1 (9.).

## Définition 5.3 ($\mathbb{N}$-modèle)

Soit $\mathcal{L}$ un langage et $N$, *Null*, *Succ*, *Plus*, *Mult* des propositions de ce langage. Un modèle $\mathcal{M}$ de ce langage est un $\mathbb{N}$-*modèle* si

$$\{a \in \mathcal{M} \mid [\![N]\!]_{x=a} = 1\} = \mathbb{N}$$

$$\{a \in \mathbb{N} \mid [\![Null]\!]_{x=a} = 1\} = \{0\}$$

$$\{(a, b) \in \mathbb{N}^2 \mid [\![Succ]\!]_{x=a, y=b} = 1\} = \{(a, b) \in \mathbb{N}^2 \mid b = a + 1\}$$

$$\{(a,b,c) \in \mathbb{N}^3 \mid [\![Plus]\!]_{x=a,y=b,z=c} = 1\} = \{(a,b,c) \in \mathbb{N}^3 \mid c = a+b\}$$
$$\{(a,b,c) \in \mathbb{N}^3 \mid [\![Mult]\!]_{x=a,y=b,z=c} = 1\} = \{(a,b,c) \in \mathbb{N}^3 \mid c = a \times b\}$$
$$\{(a,b) \in \mathbb{N}^2 \mid [\![Eq]\!]_{x=a,y=b} = 1\} = \{(a,b) \in \mathbb{N}^2 \mid a = b\}$$

Si $\mathcal{T}$ est une théorie dans le langage $\mathcal{L}$, un $\mathbb{N}$-modèle de $\mathcal{T}$ est un $\mathbb{N}$-modèle de $\mathcal{L}$ qui est, par ailleurs, un modèle de $\mathcal{T}$.

Les axiomes de la théorie $\mathcal{T}_0$ sont valides dans tous les $\mathbb{N}$-modèles.

On peut alors démontrer la proposition suivante.

## Proposition 5.3

Soit $\mathcal{L}$ un langage, $N$, *Null*, *Succ*, *Plus*, *Mult* et *Eq* des propositions de ce langage 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 $\mathcal{M}$. Alors, si $f$ est un programme et $A$ la proposition représentant $f$, les trois propositions suivantes sont équivalentes

- $f$ prend la valeur $q$ en $p_1, \ldots, p_n$,
- la proposition

$$\forall x_1 \ldots \forall x_n \forall y \; ((N_{p_1}[x_1] \wedge \ldots \wedge N_{p_n}[x_n] \wedge N_q[y]) \Rightarrow A[x_1, \ldots, x_n, y])$$

  est démontrable dans la théorie $\mathcal{T}$,
- cette proposition est valide dans le modèle $\mathcal{M}$.

*Démonstration.* On suppose que $f$ prend la valeur $q$ en $p_1, \ldots, p_n$ et on montre, par récurrence sur la structure de $f$, que la proposition

$$\forall x_1 \ldots \forall x_n \forall y \; ((N_{p_1}[x_1] \wedge \ldots \wedge N_{p_n}[x_n] \wedge N_q[y]) \Rightarrow A[x_1, \ldots, x_n, y])$$

est démontrable dans $\mathcal{T}$.

- Si $f = \pi_i^n$ alors $A = Eq[y, x_i]$ et la proposition

$$\forall x_1 \ldots \forall x_n \forall y \; ((N_{p_1}[x_1] \wedge \ldots \wedge N_{p_n}[x_n] \wedge N_{p_i}[y]) \Rightarrow Eq[x_i, y])$$

  est une conséquence de la proposition 5.1 (3.). On procède de même pour le programme zéro, le successeur, l'addition et la multiplication en utilisant la proposition 5.1 (4.) et (5.).
- Si $f = \chi_{\leq}$, et $p_1 \leq p_2$, alors, d'après la proposition 5.1 (6.), la proposition $Inf[x_1, x_2]$ est démontrable sous les hypothèses $N_{p_1}[x_1]$ et $N_{p_2}[x_2]$. La proposition $\exists z' \; (Null[z'] \wedge Succ[z', y])$, quant à elle, est démontrable sous l'hypothèse $N_1[y]$ et donc la proposition $A$ est démontrable sous les hypothèses $N_{p_1}[x_1]$, $N_{p_2}[x_2]$ et $N_1[y]$. On procède de même en utilisant la proposition 5.1 (7.) dans le cas où $p_2 < p_1$.

- Si $f = \circ_m^n(h, g_1, \ldots, g_m)$, alors comme $f$ termine en $(p_1, \ldots, p_n)$, $g_1$, ..., $g_m$ terminent en $(p_1, \ldots, p_n)$ et si on appelle $r_i$ le nombre $g_i(p_1, \ldots, p_n)$, $h$ termine en $r_1, \ldots, r_m$ et $q = h(r_1, \ldots, r_m)$. Soient $B_1, \ldots, B_m$ et $C$ les propositions représentant les programmes $g_1, \ldots, g_m$ et $h$. Par hypothèse de récurrence, sous les hypothèses $N_{p_1}[x_1]$, ..., $N_{p_n}[x_n]$, $N_{r_1}[w_1]$, ..., $N_{r_m}[w_m]$ et $N_q[y]$, les propositions $B_1[x_1, \ldots, x_n, w_1]$, ..., $B_m[x_1, \ldots, x_n, w_m]$ et $C[w_1, \ldots, w_m, y]$ sont démontrables et d'après la proposition 5.1 (1.), sous ces mêmes hypothèses, les propositions $N[w_1]$, ..., $N[w_n]$ sont démontrables. On en déduit que la proposition $A$ est démontrable. On élimine les hypothèses $N_{r_1}[w_1]$, ..., $N_{r_m}[w_m]$ en utilisant la proposition 5.1 (2.).
- Si $f = \mu^n(g)$ alors, comme $f$ termine en $(p_1, \ldots, p_n)$ et vaut $q$, $g$ termine en $(p_1, \ldots, p_n, 0)$, ..., $(p_1, \ldots, p_n, q-1)$ et prend une valeur non nulle et $g$ est définie en $(p_1, \ldots, p_n, q)$ et prend la valeur 0. Il existe donc des entiers $r_0, \ldots, r_{q-1}$ tels que $g(p_1, \ldots, p_n, 0) = r_0 + 1$, ..., $g(p_1, \ldots, p_n, q-1) = r_{q-1} + 1$.
  Soit $B$ la proposition représentant le programme $g$. Par hypothèse de récurrence, sous les hypothèses $N_{p_1}[x_1]$, ..., $N_{p_n}[x_n]$ et $N_q[y]$, pour tout $i$ compris entre 0 et $q-1$, les propositions

$$\forall v \forall w \ ((N_i[v] \wedge N_{r_i+1}[w]) \Rightarrow B[x_1, \ldots, x_n, v, w])$$

  sont démontrables. En utilisant la proposition 5.1 (1.) et (2.), on en déduit que la proposition

$$\forall v \ (N_i[v] \Rightarrow \exists w \exists w' \ (N[w'] \wedge \mathit{Succ}[w', w] \wedge B[x_1, \ldots, x_n, v, w]))$$

  est démontrable. Avec la proposition 5.2, on en déduit que la proposition

$$\forall v \ (\mathit{InfS}[v, y] \Rightarrow \exists w \exists w' \ (N[w'] \wedge \mathit{Succ}[w', w] \wedge B[x_1, \ldots, x_n, v, w]))$$

  est démontrable. De même la proposition

$$\forall w \ (\mathit{Null}[w] \Rightarrow B[x_1, \ldots, x_n, y, w])$$

  est démontrable. On en conclut que la proposition $A$ est démontrable.

Le modèle $\mathcal{M}$ étant un modèle de la théorie $\mathcal{T}$, si la proposition

$$\forall x_1 \ldots \forall x_n \forall y \ ((N_{p_1}[x_1] \wedge \ldots \wedge N_{p_n}[x_n] \wedge N_q[y]) \Rightarrow A[x_1, \ldots, x_n, y])$$

est démontrable dans $\mathcal{T}$ elle est valide dans le modèle $\mathcal{M}$.

Enfin, si la proposition

$$\forall x_1 \ldots \forall x_n \forall y \ ((N_{p_1}[x_1] \wedge \ldots \wedge N_{p_n}[x_n] \wedge N_q[y]) \Rightarrow A[x_1, \ldots, x_n, y])$$

est valide dans $\mathcal{M}$, il existe des entiers $p_1, \ldots, p_n, q$ tels que

$$[\![A[x_1, \ldots, x_n, y]]\!]_{x_1=p_1,\ldots,x_n=p_n,y=q} = 1$$

et, en utilisant le fait que $\mathcal{M}$ est un $\mathbb{N}$-modèle, on montre, par récurrence sur la structure de $f$, que $f$ prend la valeur $q$ en $p_1, \ldots, p_n$.

## 5.3 Le théorème de Church

### Définition 5.4

Soit $f$ un programme et $A$ la proposition représentant ce programme. La proposition « Le programme $f$ termine en $p_1, \ldots, p_n$ » est la proposition close

$$\forall x_1 \ldots \forall x_n \ ((N_{p_1}[x_1] \wedge \ldots \wedge N_{p_n}[x_n]) \Rightarrow \exists y \ (N[y] \wedge A[x_1, \ldots, x_n, y]))$$

### Proposition 5.4

Soit $\mathcal{L}$ un langage, $N$, *Null*, *Succ*, *Plus*, *Mult* et *Eq* des propositions de ce langage 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 $\mathcal{M}$. Alors, si $f$ est un programme, les trois propositions suivantes sont équivalentes

- le programme $f$ termine en $p_1, \ldots, p_n$,
- la proposition « Le programme $f$ termine en $p_1, \ldots, p_n$ » est démontrable dans $\mathcal{T}$,
- cette proposition est valide dans $\mathcal{M}$.

*Démonstration.* Si le programme $f$ termine en $p_1, \ldots, p_n$ alors il existe un entier $q$ tel que $f$ prenne la valeur $q$ en $p_1, \ldots, p_n$. D'après la proposition 5.3, la proposition

$$\forall x_1 \ldots \forall x_n \forall y \ ((N_{p_1}[x_1] \wedge \ldots \wedge N_{p_n}[x_n] \wedge N_q[y]) \Rightarrow A[x_1, \ldots, x_n, y])$$

est démontrable dans $\mathcal{T}$. On en déduit, en utilisant la proposition 5.1 (1.) et (2.), que la proposition $\forall x_1 \ldots \forall x_n \ ((N_{p_1}[x_1] \wedge \ldots \wedge N_{p_n}[x_n]) \Rightarrow \exists y \ (N[y] \wedge A[x_1, \ldots, x_n, y]))$ est démontrable dans $\mathcal{T}$.

Le modèle $\mathcal{M}$ étant un modèle de la théorie $\mathcal{T}$, si cette proposition est démontrable dans $\mathcal{T}$ elle est valide dans le modèle $\mathcal{M}$.

Enfin si cette proposition est valide dans $\mathcal{M}$, il existe un entier $q$ tel que

$$[\![A[x_1, \ldots, x_n, y]]\!]_{x_1=p_1,\ldots,x_n=p_n,y=q} = 1$$

La proposition

$$\forall x_1 \ldots \forall x_n \forall y \ ((N_{p_1}[x_1] \wedge \ldots \wedge N_{p_n}[x_n] \wedge N_q[y]) \Rightarrow A[x_1, \ldots, x_n, y])$$

est donc valide dans $\mathcal{M}$. D'après la proposition 5.3, $f$ prend la valeur $q$ en $p_1, \ldots, p_n$ et termine donc en $p_1, \ldots, p_n$.

### Proposition 5.5

La fonction $T$ associant au numéro d'un programme $f$ et à $p_1, \ldots, p_n$, le numéro de la proposition « Le programme $f$ termine en $p_1, \ldots, p_n$ » et prenant la valeur 0 sur les entiers qui ne sont pas le numéro d'un programme est calculable.

*Démonstration.* Cette fonction est définie par récurrence bien fondée.

Nous obtenons ainsi un premier résultat d'indécidabilité de la démontrabilité.

### Proposition 5.6

Soit $\mathcal{L}$ un langage, *N*, *Null*, *Succ*, *Plus*, *Mult* et *Eq* des propositions de ce langage 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. Alors l'ensemble des propositions closes de $\mathcal{L}$ démontrables dans $\mathcal{T}$ est indécidable.

*Démonstration.* S'il existait une fonction calculable $F$ associant 1 ou 0 au numéro d'une proposition selon que cette proposition est démontrable dans $\mathcal{T}$ ou non, la fonction $F \circ T$ serait calculable, en contradiction avec le théorème d'indécidabilité du problème de l'arrêt.

Nous montrons ensuite que l'hypothèse, selon laquelle la théorie $\mathcal{T}$ doit démontrer les axiomes de la théorie $\mathcal{T}_0$, est superflue.

### Proposition 5.7

Soit $\mathcal{L}$ un langage, *N*, *Null*, *Succ*, *Plus*, *Mult* et *Eq* des propositions de ce langage et $\mathcal{T}$ une théorie dans ce langage qui a un $\mathbb{N}$-modèle. Alors, l'ensemble des propositions closes de $\mathcal{L}$ démontrables dans la théorie $\mathcal{T}$ est indécidable.

*Démonstration.* La théorie $\mathcal{T} \cup \mathcal{T}_0$ démontre les axiomes de $\mathcal{T}_0$ et elle a un $\mathbb{N}$-modèle. D'après la proposition 5.6, la démontrabilité dans cette théorie est donc indécidable.

On utilise ensuite, encore une fois, une réduction. Soit $H$ la conjonction des axiomes de la théorie $\mathcal{T}_0$. La proposition $H \Rightarrow A$ est démontrable dans la théorie $\mathcal{T}$ si et seulement si la proposition $A$ est démontrable dans la théorie $\mathcal{T} \cup \mathcal{T}_0$. Soit $T$ la fonction qui associe le numéro de la proposition $H \Rightarrow A$ au numéro de la proposition $A$. La fonction $T$ est calculable et la proposition de numéro $T(\ulcorner A \urcorner)$ est démontrable dans la théorie $\mathcal{T}$ si et seulement si la proposition $A$ est démontrable dans $\mathcal{T} \cup \mathcal{T}_0$. S'il existait un algorithme de décision $F$ pour la théorie $\mathcal{T}$, $F \circ T$ serait un algorithme de décision pour $\mathcal{T} \cup \mathcal{T}_0$ en contradiction avec le fait que $\mathcal{T} \cup \mathcal{T}_0$ est indécidable.

### Proposition 5.8

Soit $\mathcal{L}$ un langage, *N*, *Null*, *Succ*, *Plus*, *Mult* et *Eq* des propositions de ce langage. Si $\mathcal{L}$ a un $\mathbb{N}$-modèle, alors l'ensemble des propositions closes de $\mathcal{L}$ démontrables dans la théorie vide est indécidable.

*Démonstration.* D'après 5.7, en prenant $\mathcal{T} = \varnothing$.

### Théorème 5.1 (L'indécidabilité de l'arithmétique)

L'ensemble des propositions closes démontrables dans l'arithmétique, ou dans n'importe quelle extension de l'arithmétique qui a $(\mathbb{N}, 0, x \mapsto x + 1, +, \times, =)$ pour modèle, est indécidable.

*Démonstration.* On pose $N = \top$, $Null = (x = 0)$, $Succ = (y = S(x))$, $Plus = (z = x + y)$, $Mult = (z = x \times y)$ et $Eq = (x = y)$. Le modèle $\mathbb{N}$ est un $\mathbb{N}$-modèle. On peut donc appliquer la proposition 5.7.

On peut généraliser ce théorème à toutes les extensions cohérentes de l'arithmétique, c'est-à-dire à toutes les extensions de l'arithmétique qui ont un modèle, que ce modèle soit $\mathbb{N}$ ou non, ce qui permet de montrer également l'indécidabilité d'extensions exotiques de l'arithmétique qui, comme celles que l'on a construites dans la démonstration du théorème de Löwenheim-Skolem, sont cohérentes sans avoir $\mathbb{N}$ pour modèle. Mais on ne le fera pas ici. Il est cependant important de remarquer que ce résultat ne s'étend pas aux extensions contradictoires de l'arithmétique. Si on ajoute l'axiome $\bot$ par exemple, alors toutes les propositions sont démontrables et la théorie devient alors trivialement décidable.

## Théorème 5.2 (Church)

Soit un langage contenant au moins un symbole de prédicat binaire, alors l'ensemble des propositions closes démontrables dans la théorie vide dans ce langage est indécidable.

*Démonstration.* On démontre que l'on peut définir des propositions $N$, *Null*, *Succ*, *Plus*, *Mult* et $Eq$ et un $\mathbb{N}$-modèle $\mathcal{M}$ de ce langage et on conclut avec la proposition 5.8. Soit $\mathcal{M} = \mathbb{N} \uplus (\mathbb{N} \times \mathbb{N})$. On pose $\hat{R} = \{(a,(a,b)) \mid a \in \mathbb{N}, b \in \mathbb{N}\} \cup \{((a,b),b) \mid a \in \mathbb{N}, b \in \mathbb{N}\} \cup \{((a,b),(a+b,a\times b)) \mid a \in \mathbb{N}, b \in \mathbb{N}\}$. On définit les propositions

$$Eq = \forall z\ (x\ R\ z \Leftrightarrow y\ R\ z)$$

$$N = \exists y_1 \exists y_2 \exists y_3\ (\neg Eq[y_1,y_2] \wedge \neg Eq[y_1,y_3] \wedge \neg Eq[y_2,y_2] \wedge x\ R\ y_1 \wedge x\ R\ y_2 \wedge x\ R\ y_3)$$

$$Plus = N[x] \wedge N[y] \wedge N[z] \wedge \exists w \exists w'\ (x\ R\ w \wedge w\ R\ y \wedge w\ R\ w' \wedge z\ R\ w')$$

$$Mult = N[x] \wedge N[y] \wedge N[z] \wedge \exists w \exists w'\ (x\ R\ w \wedge w\ R\ y \wedge w\ R\ w' \wedge w'\ R\ z)$$

$$Null = N[x] \wedge \forall y\ (N[y] \Rightarrow Plus[x,y,y])$$

$$Un = N[x] \wedge \forall y\ (N[y] \Rightarrow Mult[x,y,y])$$

$$Succ = \exists u\ (Un[u] \wedge Plus[x,u,y])$$

Il n'est pas difficile de montrer que $[\![Eq[x,y]]\!]_{x=u,y=v} = 1$ si et seulement si $u = v$ en distinguant successivement le cas où $u$ est un entier et celui ou c'est un couple, que $[\![N[x]]\!]_{x=u} = 1$ si et seulement si $u$ est un entier, que $[\![Plus[x,y,z]]\!]_{x=p,y=q,z=r} = 1$ si et seulement si $p$, $q$ et $r$ sont des entiers et $p+q=r$, que $[\![Mult[x,y,z]]\!]_{x=p,y=q,z=r} = 1$ si et seulement si $p$, $q$ et $r$ sont des entiers et $p \times q = r$, que $[\![Null[x]]\!]_{x=p} = 1$ si et seulement si $p = 0$, et que $[\![Succ[x,y]]\!]_{x=p,y=q} = 1$ si et seulement si $p$ et $q$ sont des entiers et $p+1=q$.

Si le langage $\mathcal{L}$ contient un prédicat d'arité $n$ pour $n \geq 2$, la construction d'un $\mathbb{N}$-modèle se généralise simplement. Un langage qui contient au moins un symbole de prédicat unaire $P$ et un symbole de fonction $f$ d'arité $n \geq 2$ est également indécidable, car avec un symbole de prédicat unaire $P$ et un symbole de prédicat $n$-aire $f$ on peut construire la proposition $P(f(x_1,\ldots,x_n))$ qui simule un symbole de prédicat $n$-aire.

Restent le cas où tous les symboles de prédicat sont d'arité nulle — auquel cas peu importent les symboles de fonction qui ne peuvent pas être utilisés dans les propositions — et celui où tous les symboles de fonction et de prédicat sont au plus unaire. On peut montrer que la démontrabilité est décidable dans ces deux cas.

Le théorème de Church permet d'apprécier la révolution qu'a constituée l'introduction par G. Frege de prédicats binaires. Toutes les logiques antérieures

— la logique des syllogismes d'Aristote, ... — qui ne comportent que des symboles au plus unaires — Homme, Mortel, ... — sont décidables.

Il faut prendre garde au fait que, bien que la démontrabilité dans la logique des prédicats dans un langage contenant au moins un symbole de prédicat binaire soit indécidable, en ajoutant des axiomes, on peut rendre la démontrabilité décidable. C'est naturellement le cas si on ajoute l'axiome $\bot$, puisqu'une théorie contradictoire est trivialement décidable, mais c'est par exemple aussi le cas si on ajoute l'axiome $\forall x \forall y\ (x\ R\ y)$ qui est cohérent. Le théorème de Church ne condamne donc pas *a priori* la recherche d'algorithmes pour des théories particulières, à condition que celles-ci n'aient pas de $\mathbb{N}$-modèle, même si elles utilisent un symbole de prédicat binaire. Ainsi, A. Tarski a démontré que la géométrie élémentaire est décidable, bien qu'elle utilise de nombreux prédicats binaires. Nous verrons, au chapitre 7, un autre exemple de théorie décidable.

Pour terminer cette section, mentionnons une autre généralisation du théorème d'indécidabilité de l'arithmétique. Nous avons vu que, quand nous nous donnons un programme $f$ et des entiers $p_1, \ldots, p_n$, nous pouvons construire une proposition close de l'arithmétique qui est démontrable si et seulement si le programme $f$ termine en $p_1, \ldots, p_n$. En 1970, Y. Matiyasevich a montré qu'il est possible de construire une telle proposition de la forme $\exists z_1 \ldots \exists z_m\ (t = u)$. De ce fait, l'ensemble des propositions de la forme $\exists z_1 \ldots \exists z_m\ (t = u)$ démontrables dans l'arithmétique est indécidable. Or, une proposition de cette forme exprime simplement l'existence d'une solution dans le domaine des entiers pour l'équation polynomiale à coefficients entiers $t = u$. De ce fait, il n'existe pas d'algorithme permettant de décider si une équation polynomiale à coefficients entiers a une solution dans le domaine des entiers ou non. Ce théorème résout, par la négative, un problème posé par D. Hilbert en 1900 (*le dixième problème de Hilbert*) : trouver un algorithme qui indique si une équation polynomiale à plusieurs variables et à coefficients entiers a une solution dans le domaine des entiers ou non. La construction d'une proposition de la forme $\exists z_1 \ldots \exists z_m\ (t = u)$ a cependant demandé un peu de travail, puisque si le lien entre le théorème de Church et une potentielle solution négative du dixième problème de Hilbert avait été entrevu en 1953 par M. Davis, qui avait proposé une première simplification de la forme des propositions représentant les programmes, ce n'est qu'en 1970 que la construction a été achevée par Matiyasevich.

## 5.4 La semi-décidabilité

Si l'ensemble des propositions démontrables dans la logique des prédicats est indécidable, on peut, en revanche, montrer que les règles de déduction sont effectives et donc en déduire, en utilisant la proposition 3.14, que l'ensemble des propositions démontrables est semi-décidable. Ce résultat s'étend à toutes les théories formées d'un nombre fini d'axiomes et même à toutes celles dont l'ensemble des axiomes est décidable.

Afin de préparer la démonstration de la proposition 5.10, nous redonnons ici la démonstration de cette proposition en partant de la proposition 3.13.

### Proposition 5.9

Soit $\mathcal{T}$ une théorie dont l'ensemble des axiomes est décidable, les propositions démontrables dans $\mathcal{T}$ forment un ensemble semi-décidable.

*Démonstration.* Les règles de déduction étant effectives, d'après la proposition 3.13, l'ensemble des démonstrations est décidable. Et l'ensemble des axiomes de la théorie $\mathcal{T}$ étant décidable, on peut construire une fonction calculable $g$ qui prend en argument le numéro d'un arbre $\pi$ et le numéro d'une proposition $A$, vérifie que $\pi$ est une démonstration bien formée, que sa racine est un séquent $\Gamma \vdash B$ tel que $B = A$ et tel que tous les éléments de $\Gamma$ soient des axiomes de $\mathcal{T}$. La fonction $h$ définie par $h(A)$ est le plus petit entier $\pi$ tel que $1 \dot{-} g(\pi, A) = 0$ composée avec la fonction constante égale à 1 est un algorithme de semi-décision pour l'ensemble des propositions démontrables dans la théorie $\mathcal{T}$. Si $A$ est démontrable dans $\mathcal{T}$, alors $h(A) = 1$, sinon $h$ n'est pas définie en $A$.

L'ensemble des démonstrations est donc un ensemble décidable et celui des propositions démontrables un ensemble semi-décidable. Ces deux résultats sont à l'origine de la conception de deux types de programmes informatiques : les *programmes de vérification de démonstrations* et les *programmes de démonstration automatique*. Les programmes de la première catégorie prennent en entrée un arbre $\pi$, ils terminent toujours et indiquent si $\pi$ est une démonstration bien formée ou non. Les programmes de la seconde catégorie, dont nous verrons un exemple au chapitre 6, prennent en entrée une proposition $A$ et recherchent une démonstration $\pi$ de cette proposition. Quand la proposition n'est pas démontrable, cette recherche se poursuit à l'infini.

## 5.5 Le premier théorème d'incomplétude de Gödel

La construction des fonctions $g$ et $h$ dans la démonstration de la proposition 5.9 mène à se demander ce qu'il se passe si on modifie la définition de la fonction $h$, en une fonction $h'$, de manière à rechercher simultanément une démonstration de la proposition $A$ et de la proposition $\neg A$ dans la théorie $\mathcal{T}$, et à retourner 1 ou 0 selon que l'on a trouvé une démonstration de l'une ou l'autre proposition. Chacune des propositions $A$ et $\neg A$ pouvant être démontrable ou non, quatre cas peuvent se produire

1. les proposition $A$ et $\neg A$ sont toutes les deux démontrables,
2. la proposition $A$ est démontrable, mais pas $\neg A$,
3. la proposition $\neg A$ est démontrable, mais pas $A$,
4. ni la proposition $A$ ni la proposition $\neg A$ ne sont démontrables.

Si on suppose la théorie $\mathcal{T}$ cohérente, aucune proposition n'est dans le cas (1.), dans le cas numéro (2.), $h'(A) = 1$, dans le cas numéro (3.), $h'(A) = 0$ et dans le cas numéro (4.), $h'$ n'est pas définie en $A$.

Il est facile de donner des exemples de propositions qui sont dans le cas (2.) et de propositions qui sont dans le cas (3.), mais on peut s'interroger sur l'existence de propositions qui sont dans le cas (4.). Existe-t-il des propositions $A$ telles que ni $A$ ni $\neg A$ ne soient démontrables dans la théorie $\mathcal{T}$ ?

On montre par l'absurde que la réponse est positive dans toutes les théories dans lesquelles l'ensemble des propositions démontrables est indécidable : s'il n'existait pas de propositions dans le cas (4.), la fonction $h'$ serait un algorithme de décision pour la démontrabilité dans la théorie $\mathcal{T}$, or, par hypothèse, un tel algorithme n'existe pas.

### Définition 5.5 (Théorie complète)

Soit $\mathcal{L}$ un langage. Une théorie $\mathcal{T}$, exprimée dans $\mathcal{L}$, est dite *complète* si pour toute proposition close $A$ de $\mathcal{L}$, $A$ est démontrable dans $\mathcal{T}$ ou $\neg A$ est démontrable dans $\mathcal{T}$.

### Proposition 5.10

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. Alors, la théorie $\mathcal{T}$ est incomplète : il existe une proposition close $G$ telle que ni $G$ ni $\neg G$ ne soient démontrables dans cette théorie.

*Démonstration.* Soit $g$ la fonction calculable qui au numéro d'un arbre $\pi$ et au numéro d'une proposition close $A$ associe la valeur 1 si $\pi$ est une démonstration bien formée dont la racine est un séquent $\Gamma \vdash B$ tel que $B = A$ et tous les éléments de $\Gamma$ sont des axiomes de $\mathcal{T}$, et la valeur 0 sinon. Soit $r$ la fonction calculable qui à une démonstration, dont la racine est un séquent $\Gamma \vdash B$, associe la proposition $B$. Soit $\hat{\neg}$ la fonction qui associe le numéro de la proposition $\neg A$ à celui de la proposition $A$ : $\hat{\neg}(x) = \ulcorner\neg\urcorner; (x; 0)$. Soit $\mid$ la fonction *ou* sur les booléens : $x \mid y = x + y \dot{-} (x \times y)$ et $\chi_=$ la fonction caractéristique de l'égalité. Soit $h_1$ la fonction calculable définie par $h_1(A)$ est le plus petit entier $\pi$ tel que $1 \dot{-} (g(\pi, A) \mid g(\pi, \hat{\neg}(A))) = 0$. Soit $h'$ la fonction $h'(A) = \chi_=(r(h_1(A)), A)$.

Si la théorie $\mathcal{T}$ était complète, $h'$ serait un algorithme de décision pour la démontrabilité dans $\mathcal{T}$ en contradiction avec la proposition 5.7.

## Théorème 5.3 (Le premier théorème d'incomplétude de Gödel)

L'arithmétique et toutes ses extensions qui ont $(\mathbb{N}, 0, x \mapsto x+1, +, \times, =)$ comme modèle et dont l'ensemble des axiomes est décidable sont incomplètes.

*Démonstration.* On pose $N = \top$, $Null = (x = 0)$, $Succ = (y = S(x))$, $Plus = (z = x + y)$, $Mult = (z = x \times y)$ et $Eq = (x = y)$. L'ensemble des axiomes de la théorie est décidable et le modèle $\mathbb{N}$ est un $\mathbb{N}$-modèle de la théorie. On peut donc appliquer la proposition 5.10.

On peut généraliser ce théorème à toutes les extensions cohérente de l'arithmétique, c'est-à-dire à toutes les extensions de l'arithmétique dont l'ensemble des axiomes est décidable et qui ont un modèle, que ce modèle soit $\mathbb{N}$ ou non, ce qui permet de montrer également l'incomplétude d'extensions exotiques de l'arithmétique, qui sont cohérentes sans avoir $\mathbb{N}$ pour modèle. Mais on ne le fera pas ici.

Il est cependant important de remarquer que ce résultat ne s'étend pas aux extensions contradictoires de l'arithmétique. Si on ajoute l'axiome $\bot$, par exemple, alors toutes les propositions sont démontrables et la théorie est alors trivialement complète. Ce résultat ne s'étend pas non plus aux extensions de l'arithmétique dont l'ensemble d'axiomes est indécidable. Ainsi, la théorie dont les axiomes sont toutes les propositions valides dans le modèle $\mathbb{N}$ est un exemple d'extension de l'arithmétique cohérente et complète. Mais le théorème 5.3 montre que l'ensemble des axiomes de cette théorie est indécidable. De même, dans la démonstration de la proposition 2.5, on montre que toute théorie $\mathcal{T}$ a une extension cohérente et complète $\mathcal{U}$, mais, en général, l'ensemble des axiomes de cette théorie n'est pas décidable.

## Exercice 5.1 (Un exemple de proposition indéterminée)

La proposition 5.10 montre qu'il existe une proposition close $G$, telle que ni $G$ ni $\neg G$ ne soient démontrables dans la théorie $\mathcal{T}$, mais ne donne pas d'exemple d'une telle proposition. On montre dans cet exercice que l'on peut la modifier de manière à construire une telle proposition.

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 $n = \ulcorner \pi \urcorner$, $p = \ulcorner A \urcorner$ et l'arbre $\pi$ est une démonstration 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. On écrit $F[t_1,t_2,t_3,u]$ la proposition $(t_1/x_1, t_2/x_2, t_3/x_3, u/y)F$.

D'après la proposition 5.3, les trois propositions suivantes sont équivalentes

- $f(n,p,q) = r$,
- la proposition

$$\forall x_1 \forall x_2 \forall x_3 \forall y\ (N_n[x_1] \wedge N_p[x_2] \wedge N_q[x_3] \wedge N_r[y] \Rightarrow F[x_1,x_2,x_3,y])$$

  est démontrable dans $\mathcal{T}'$,
- dans le modèle $\mathcal{M}$, $[\![F]\!]_{x_1=n,x_2=p,x_3=q,x_4=r} = 1$.

Soit $T$ la proposition

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

$m = \ulcorner T \urcorner$ et $G$ la proposition close

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

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 $n$, $f(n,m,m) = 0$,
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 la proposition $G$ n'est pas démontrable dans $\mathcal{T}'$.
En déduire que la proposition $G$ n'est pas démontrable dans $\mathcal{T}$.
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 la proposition $\neg G$ n'est pas démontrable dans $\mathcal{T}'$.
En déduire que la proposition $\neg G$ n'est pas démontrable dans $\mathcal{T}$.

## Exercice 5.2

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.

1. 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.
2. Montrer que la proposition $\forall x_1 \ldots \forall x_m\ \neg(t = u)$ n'est pas démontrable.
3. 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. 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. Montrer que si $a$ et $b$ sont deux termes clos de l'arithmétique, alors la proposition $a = b$ est démontrable ou la proposition $\neg(a = b)$ est démontrable.
4. 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 $(\underline{p_1}/x_1, \ldots, \underline{p_m}/x_m)(t = u)$ 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 $(\underline{p_1}/x_1, \ldots, \underline{p_m}/x_m)(t = u)$ n'est pas démontrable.
5. 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 $(\underline{p_1}/x_1, \ldots, \underline{p_m}/x_m)\neg(t = u)$ est démontrable.
6. 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 tous $p_1, \ldots, p_m$ la proposition $(\underline{p_1}/x_1, \ldots, \underline{p_m}/x_m)A$ est démontrable,
   - la proposition $\forall x_1 \ldots \forall x_m\ A$ n'est pas démontrable.