Alexandre DIKOVSKY
Université de Nantes

Logique Mathématique pour l'Informatique

Cours 9. Théories du 1^{er} ordre.

9.1. Trois types de théories.

Une théorie du 1^{er} ordre est un ensemble de **propositions** du 1^{er} ordre.

Soit $\mathcal{A}$ une théorie du 1^{er} ordre dans une signature Σ. Il y a deux façons d'obtenir les conséquences de $\mathcal{A}$:

- théorie axiomatique sémantique de $\mathcal{A}$:

$$Th^1(\mathcal{A}, \Sigma) = \{\phi \in \mathcal{L}^1_\Sigma \ (une\ proposition) \mid \mathcal{A} \models \phi\},$$

- théorie axiomatique formelle de $\mathcal{A}$,
définie par un système formel du 1^{er} ordre (par exemple, par le calcul naturel N) :

$$Th^1_N(\mathcal{A}, \Sigma) = \{\phi \in \mathcal{L}^1_N \ (une\ proposition) \mid \ \Gamma \ \vdash_N \ \phi \ pour\ un\ \Gamma \subseteq \mathcal{A}\ fini\}.$$

Remarque. Nous allons omettre Σ quand elle est implicite : $Th^1(\mathcal{A})$, $Th^1_N(\mathcal{A})$.

Exemple 1. *Théorie de l'égalité dans une signature Σ ($= /2 \in \Sigma_p$).*
$\mathbf{eq}_\Sigma$: (e_1) $\forall x\ (x = x)$
(e_2) $\overline{\forall}\ (x_1 = y_1 \wedge ... \wedge x_n = y_n \rightarrow f(x_1, ..., x_n) = f(y_1, ..., y_n))$
(pour tout $f/n \in \Sigma_f$)
(e_3) $\overline{\forall}\ (x_1 = y_1 \wedge ... \wedge x_n = y_n \rightarrow (p(x_1, ..., x_n) \rightarrow p(y_1, ..., y_n)))$
(pour tout $p/n \in \Sigma$, $= /2$ inclu).
Par exemple, on peut prouver que les formules

$$\phi_{sme} \mathrel{\hat{=}} \forall x, y\ (x = y \rightarrow y = x),$$
$$\phi_{tre} \mathrel{\hat{=}} \forall x, y, z\ (x = y \wedge y = z \rightarrow x = z)$$

sont conséquences logiques de $\mathbf{eq}_\Sigma$: $\mathbf{eq}_\Sigma \models \phi_{sme}$, $\mathbf{eq}_\Sigma \models \phi_{tre}$. Autrement dit, $\phi_{sme}, \phi_{tre} \in Th^1(\mathbf{eq}_\Sigma)$ pour tous Σ.

Exemple 2. *Soit*

$$\mathbf{gr} = \{x * (y * z) = (x * y) * z,\ x * x^{-1} = 1, x * 1 = x\}\ (théorie\ des\ groupes)$$

Alors :

$$x^{-1} * x = 1, 1 * x = x * 1, (x * y)^{-1} = y^{-1} * x^{-1} \in Th^1(\mathbf{gr} \cup \mathbf{eq}_{\mathbf{gr}})$$

c'est-à-dire, $\mathbf{gr} \cup \mathbf{eq}_{\mathbf{gr}} \models x^{-1} * x = 1, 1 * x = x * 1, (x * y)^{-1} = y^{-1} * x^{-1}$.

Exemple 3. *Soit la théorie* **FM** *:*
$(p\grave{e}re(x,y) \ \vee \ m\grave{e}re(x,y)) \ \wedge \ sexe(y,m) \rightarrow fils(y,x)$
$(p\grave{e}re(x,y) \ \vee \ m\grave{e}re(x,y)) \ \wedge \ sexe(y,f) \rightarrow fille(y,x)$
$fr\grave{e}re(x,y) \leftrightarrow sexe(x,m) \ \wedge \ \exists z \ (p\grave{e}re(z,x) \ \wedge \ p\grave{e}re(z,y) \ \vee \ m\grave{e}re(z,x) \ \wedge \ m\grave{e}re(z,y))$.
Alors :

$$\mathbf{FM} \cup \{fr\grave{e}re(paule, pauline), \neg sexe(pauline, m)\} \models \exists z \ (fille(pauline, z)).$$

Question : Quelle est la théorie $Th^1(\emptyset)$? Par exemple, $\forall x \ (p(x) \rightarrow (q(x) \rightarrow p(x) \wedge q(x))) \in Th^1(\emptyset)$.

Une autre manière de définir une théorie logique est de fixer un modèle (contexte) particulier M sur Σ et de considérer comme théorie l'ensemble de toutes propositions vraies dans ce modèle :

- théorie d'une classe $\mathcal{M}$ de modèles de Σ :

$$Tm^1(\mathcal{M}) = \{\phi \in \mathcal{L}^1 \ (\textit{une proposition}) \mid M \models \phi \textit{ pour tout } M \in \mathcal{M}\}.$$

En particulier, si $\mathcal{M}$ consiste en un seul modèle M, on écrit $Tm^1(M)$.

Selon cette définition, $Tm^1(\mathcal{M}) = \bigcap_{M \in \mathcal{M}} Tm^1(M)$.

Exemple 4. *Soit* $\Sigma_{ar} = (\{= /2\}, \{'/1, \ +/2, \ */2, \ \mathbf{0}/0\})$ *la signature arithmétique, et* **Ar** *son interprétation standard, ($'/1$ étant l'opération de successeur sur Z_+). Alors,* $Tm^1(\mathbf{Ar})$ *est l'ensemble des propositions qui sont vraies en arithmétique des entiers non négatives.*

Exemple 5. $\mathcal{G}$ *étant la classe des groupes dans la signature* $\Sigma_{\mathbf{gr}}$, *sa théorie est*

$$Tm^1(\mathcal{G}, \Sigma_{\mathbf{gr}}) = \bigcap_{G \in \mathcal{G}} Tm^1(G, \Sigma_{\mathbf{gr}}),$$

où $Tm^1(G, \Sigma_{\mathbf{gr}})$ *est la théorie du groupe* G.

Remarque. Pour un ensemble de formules T, soit $\mathcal{M}_\Sigma(T) =_{df} \{M \mid M \models T\}$. Alors, par définition :

$$Th^1(T, \Sigma) = Tm^1(\mathcal{M}_\Sigma(T), \Sigma) = \bigcap_{M \models T} Tm^1(M, \Sigma).$$

Cela veut dire que

$$Th^1(T, \Sigma) \subseteq Tm^1(M, \Sigma)$$

pour tout modèle $M \models T$. Si

$$Th^1(T, \Sigma) = Tm^1(M, \Sigma),$$

alors on dit que T est une *théorie élémentaire* de M (T est une formalisation de M). Cette notion est étendue aux classes $\mathcal{M}$ de modèles.

Définition 1. *Si* $Th^1(\mathcal{A}) = Tm^1(\mathcal{M})$*, alors on dit que* $\mathcal{A}$ *est une théorie élémentaire de la classe* $\mathcal{M}$*.*

Si on n'impose pas de contrainte sur $\mathcal{A}$, alors on peut voir que $Tm^1(\mathcal{M})$ est lui-même sa propre théorie élémentaire. Mais on ne s'intéresse qu'aux théories "observables" :

Définition 2. $\mathcal{M}$ *est axiomatisable s'il existe un algorithme qui énumère sa théorie élémentaire* $\mathcal{A}$*.* $\mathcal{M}$ *est finiment axiomatisable si sa théorie élémentaire* $\mathcal{A}$ *est finie.*

La théorie axiomatique des groupes $\mathbf{Gr} \cup EQ_{gr}$ est une théorie élémentaire de groupes :

Théorème 1. $Th^1(\mathbf{Gr} \cup EQ_{gr}) = Tm^1(\mathcal{G})$*.*

On voit que les groupes sont finiment axiomatisables.

9.2. Théories axiomatiques du 1^{er} ordre.

Pour tout ensemble d'axiomes $\mathcal{A}$, le problème fondamental est celui de comparaison de ses théories sémantique et formelle :

$$Th^1(\mathcal{A}, \Sigma) \;=\; Th^1_N(\mathcal{A}, \Sigma) \;?$$

L'inclusion (déjà prouvée)

$$Th^1_N(\mathcal{A}, \Sigma) \subseteq Th^1(\mathcal{A}, \Sigma)$$

dit que N est un système formel *correct* (on dit aussi que $\vdash_N$ est correct par rapport à $\models$). L'inclusion inverse

$$Th^1(\mathcal{A}, \Sigma) \subseteq Th^1_N(\mathcal{A}, \Sigma)$$

veut dire que N est *complet* ($\vdash_N$ est complet par rapport à $\models$).

La complétude de N a été prouvée par K.Gödel.

Théorème 2. *(de complétude) [K.Gödel]*

$$Th^1_N(\mathcal{A}, \Sigma) = Th^1(\mathcal{A}, \Sigma)$$

pour tous $\mathcal{A}, \Sigma$*.*

Corollaire 1. *S'il existe un algorithme qui énumère un ensemble de propositions* $\mathcal{A}$*, alors il existe un algorithme qui énumère la théorie de* $\mathcal{A}$ *:* $Th^1(\mathcal{A})$*.*

Voici quelques idées importantes à la base de ce résultat fondamental.

Définition 3. *(1) Un ensemble d'axiomes* $\mathcal{A}$ *est N-cohérent, s'il existe une formule* ϕ *dans la signature de* $\mathcal{A}$ *telle que* $\phi \notin Th^1_N(\mathcal{A})$*.*

(2) $\mathcal{A}$ *est max-N-cohérent, s'il est N-cohérent et chaque* $\mathcal{A}' \supset \mathcal{A}$ *ne l'est pas.*

Proposition 1. *Si* $\mathcal{A}$ *est N-cohérent et* $\phi, \neg\phi \notin Th^1_N(\mathcal{A})$*, alors* $\mathcal{A} \cup \{\phi\}$ *et* $\mathcal{A} \cup \{\neg\phi\}$ *sont aussi N-cohérents.*

Proposition 2. *Si $\mathcal{A}$ est N-cohérent, alors on n'a $\phi, \neg\phi \in Th^1_N(\mathcal{A})$ pour aucune proposition ϕ.*

Proposition 3. *Si Σ est dénombrable et $\mathcal{A}$ est N-cohérent, alors il existe $\Sigma_1 \supset \Sigma$ dénombrable et $\mathcal{A}^{max} \supset \mathcal{A}$ dans Σ_1 qui est max-N-cohérent.*

A partir de $\mathcal{A}^{max}$ dans cette proposition, on peut construire un modèle dénombrable de $\mathcal{A}$:

Théorème 3. *[Lindenbaum] Si $\mathcal{A}$ est un ensemble N-cohérent de propositions dans une signature dénombrable Σ, alors il existe un modèle dénombrable H de $\mathcal{A}$ dans une signature dénombrable $\Sigma_1 \supseteq \Sigma$.*

Corollaire 2. *Une théorie est N-cohérente ssi elle est cohérente.*

Corollaire 3. *(de compacité) [Maltsev] Si chaque sous-ensemble fini d'une théorie T est cohérent, alors T l'est aussi.*

Corollaire 4. *La théorie $Th^1_N(\emptyset)$ coincïde avec l'ensemble des tautologies du 1^{er} ordre et donc est cohérente.*

Corollaire 5. *[Löwenheim, Skolem] Si une théorie T dans une signature dénombrable a un modèle M infini, alors T a un modèle dénombrable.*

Cela veut dire que le problème $\mathcal{A} \models \phi$ est au moins semi-décidable !

Les méthodes des tableaux et de résolution du 1^{er} ordre sont complètes aussi.

Théorème 4. *Pour toute théorie $\mathcal{A}$ du 1^{er} ordre,*

$$Th^1(\mathcal{A}) \;=\; Th^1_t(\mathcal{A}) \;=\; Th^1_r(\mathcal{A}).$$

9.3. Egalité.

La majorité des théories mathématiques et informatiques utilisent l'égalité. La théorie $\mathbf{eq}_\Sigma$ formalise l'égalité dans Σ. Pour utiliser les propriétés de l'égalité dans une autre théorie T dans la même signature, il faut les unir dans la théorie $Th^1(\mathbf{eq}_\Sigma \cup T, \Sigma)$. Pour une telle théorie il existe une méthode (appelée *normalisation*) qui transforme chaque modèle de $\mathbf{eq}_\Sigma \cup T$ en un modèle, où $=/2$ est interprété par l'égalité (un modèle *normal*).

Théorème 5. *Pour toute théorie Γ dans une signature Σ,*
1. une théorie $\Gamma \cup \mathbf{eq}_\Sigma$ a un modèle M ssi elle a un modèle normal.
2. $Th^1(\Gamma \cup \mathbf{eq}_\Sigma, \Sigma) =$
$\{\phi \in \mathcal{L}^1_\Sigma$ *(une proposition)* $\mid (M \models \Gamma \cup \mathbf{eq}_\Sigma$ *pour un modele normal* $M) \Rightarrow (M \models \phi)\}$.

Ce théorème donne une interprétation conventionnelle aux théories des égalités : la théorie des groupes, l'arithmétique, etc.

Exemple 6. $Th^1(\mathbf{gr} \cup \mathbf{eq_{gr}}) \subseteq Tm^1(\mathcal{G})$.

Un autre exemple : les théories arithmétiques dans la signature Σ_{ar}.

Exemple 7. *(Arithmétique de Robinson).*

$$
\begin{array}{lll}
\mathbf{R}: & (r1) & x = y \to x' = y' \\
 & (r2) & x = y \to (x+z = y+z \wedge z+x = z+y) \\
 & (r3) & x = y \to (x*z = y*z \wedge z*x = z*y) \\
 & (r4) & x' = y' \to x = y \\
 & (r5) & \neg(\mathbf{0} = x') \\
 & (r6) & \neg(x = \mathbf{0}) \to \exists y\ (x = y') \\
 & (r7) & x + \mathbf{0} = x \\
 & (r8) & x + y' = (x + y)' \\
 & (r9) & x * \mathbf{0} = \mathbf{0} \\
 & (r10) & x * y' = (x * y + x)
\end{array}
$$

On peut montrer que $\mathbf{eq}_{ar} \subseteq Th^1(\mathbf{R}) \subseteq Tm^1(\mathbf{Ar})$.

Exemple 8. *(Arithmétique de Peano).*

$$
\begin{array}{lll}
\mathbf{S}: & (s1) & \neg(\mathbf{0} = x') \\
 & (s2) & x' = y' \to x = y \\
 & (s3) & x + \mathbf{0} = x \\
 & (s4) & x + y' = (x + y)' \\
 & (s5) & x * \mathbf{0} = \mathbf{0} \\
 & (s6) & x * y' = (x * y + x) \\
 & (si) & \phi(\mathbf{0}) \to (\forall x\ (\phi(x) \to \phi(x')) \to \forall x\ \phi(x))
\end{array}
$$

(si) est l'axiome d'induction. ϕ est une métavariable qui porte sur les formules dans la signature Σ_{ar}. Alors, ce système est infini et dénombrable. Pour cette axiomatique aussi

$$\mathbf{eq}_{ar} \subseteq Th^1(\mathbf{S}) \subseteq Tm^1(\mathbf{Ar}).$$

De plus,

$$\mathbf{eq}_{ar} \subseteq Th^1(\mathbf{R}) \subseteq Tm^1(\mathbf{S}).$$

La signature arithmétique rend possible de simuler les nombres par les *numéraux*, c'est-à-dire les termes composés de la constante $\mathbf{0}$ à l'aide du foncteur $'/1$:

$$\lceil \mathbf{0} \rceil \hat{=} \mathbf{0}$$
$$\lceil n \rceil \hat{=} (...(\mathbf{0}')'...)' \ (n \text{ fois})$$

Par exemple : $\lceil 3 \rceil = \mathbf{0}'''$. $\lceil n \rceil$ est un *numéral.*
En utilisant l'axiome d'induction (si), on peut prouver les théorèmes arithmétiques par induction sur un numéral : soit $\Phi(x)$ une formule arithmétique avec une variable x libre. Pour prouver la formule $\forall x\ \Phi(x)$, il suffit de prouver la formule $\Phi(\mathbf{0})$ (*la base*) et la formule $\forall x\ (\Phi(x) \to \Phi(x'))$ (*pas d'induction*).

Effectivement :

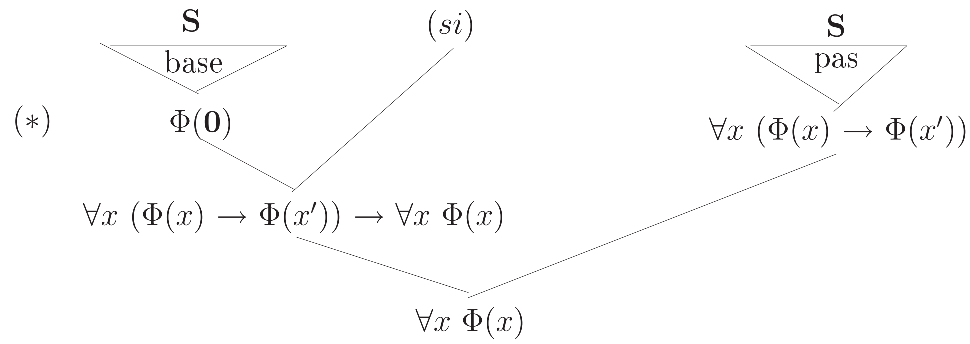

Fig. 1.

Exemple 9. *Preuve de* $\mathbf{S} \vdash_N \forall t, s\ ((t + s = \mathbf{0}) \to (t = \mathbf{0}) \wedge (s = \mathbf{0}))$ *par induction sur* s.

1. **Base** *: Une preuve de* $\Phi(\mathbf{0}) = \forall t\ ((t + \mathbf{0} = \mathbf{0}) \to (t = \mathbf{0}) \wedge (\mathbf{0} = \mathbf{0}))$ *est en Fig. 2.*

$$
\dfrac{
  \dfrac{
    \dfrac{
      [t+\mathbf{0}=\mathbf{0}]_1
      \qquad
      \dfrac{
        \dfrac{\forall x\ (x+\mathbf{0}=x)\ [s3]}{t+\mathbf{0}=t}\,\forall^-
        \qquad
        \dfrac{\forall x,y\ (x=y\rightarrow y=x)\ [\phi_{sme}\in Th^1(\mathbf{S})]}{t+\mathbf{0}=t\rightarrow t=t+\mathbf{0}}\,\forall^-\forall^-
      }{t=t+\mathbf{0}}\,\rightarrow^-
    }{t+\mathbf{0}=\mathbf{0}\wedge t=t+\mathbf{0}}\,\wedge^+
  }{t=t+\mathbf{0}\wedge t+\mathbf{0}=\mathbf{0}}\,\text{dér : comm}\wedge
  \qquad
  \dfrac{\forall x,y,z\ (x=y\wedge y=z\rightarrow x=z)\ [\phi_{tre}\in Th^1(\mathbf{S})]}{t=t+\mathbf{0}\wedge t+\mathbf{0}=\mathbf{0}\rightarrow t=\mathbf{0}}\,\forall^-\forall^-\forall^-
}{t=\mathbf{0}}
$$

$$
\dfrac{
  \dfrac{
    \dfrac{
      t=\mathbf{0}
      \qquad
      \dfrac{\forall x\ (x=x)\ [e_1\in Th^1(\mathbf{S})]}{\mathbf{0}=\mathbf{0}}\,\forall^-
    }{t=\mathbf{0}\wedge\mathbf{0}=\mathbf{0}}\,\wedge^+
  }{t+\mathbf{0}=\mathbf{0}\rightarrow t=\mathbf{0}\wedge\mathbf{0}=\mathbf{0}}\,1\ \rightarrow^+
}{\forall t\ (t+\mathbf{0}=\mathbf{0}\rightarrow t=\mathbf{0}\wedge\mathbf{0}=\mathbf{0})}\,\forall^+\ \text{(pas de } t \text{ libre dans les hypoth.)}
$$

Fig. 2.

2. **Pas d'induction** : soit $\Phi(y) =_{df} \forall t\ ((t + y = \mathbf{0}) \to (t = \mathbf{0}) \wedge (y = \mathbf{0}))$. Une preuve de $\forall y\ (\Phi(y) \to \Phi(y'))$ est en Fig. 3.

D'où selon (*), $\forall y\ \Phi(y) \in Th^1(\mathbf{S})$.

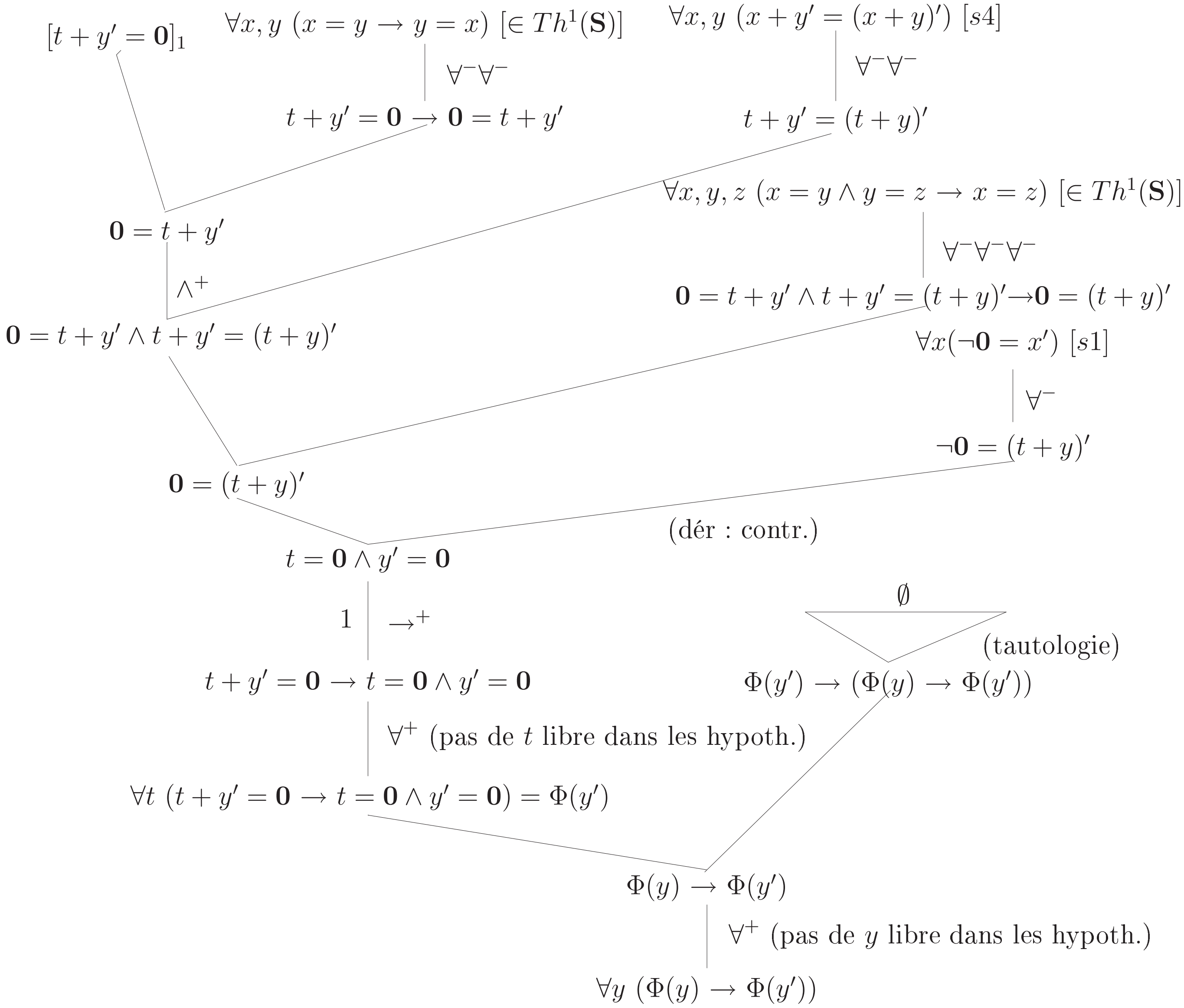

Fig. 3.

Le problème fondamental est celui de formalisation logique des théories des modèles importans, comme l'arithmétique : l'arithmétique, est-elle axiomatisable ?