Pour illustrer cette idée, supposons données deux clauses du premier ordre $C_1 = \forall \bar{x}(P(s) \vee L)$ et $C_2 = \forall \bar{y}(\neg P(t) \vee K)$. On cherche une clause du premier ordre R, telle que les instances de Herbrand de R sont exactement les clauses propositionnelles qu'on peut obtenir par résolution propositionnelle sur P entre une instance de Herbrand de C_1 et une instance de Herbrand de C_2.

On a donc

$$\begin{aligned} H(C_1) &= \{(P(s) \vee L)\sigma \mid \sigma \in \Sigma_g\} \\ H(C_2) &= \{(\neg P(t) \vee K)\tau \mid \tau \in \Sigma_g\} \end{aligned}$$

Un pas de résolution est possible ssi il existe des substitutions σ et τ telles que $s\sigma = t\tau$. Comme C_1 et C_2 peuvent être supposées ne pas partager de variables (après éventuel renommage des variables liées), $s\sigma = t\tau$ revient à dire que s et t sont unifiables.

L'ensemble des clauses closes qu'on peut obtenir par un pas de résolution est donc

$$\{L\sigma \vee K\tau \mid \sigma, \tau \in \Sigma_g, s\sigma = t\tau\} \tag{3.1}$$

Quand $\bar{x} \cap \bar{y} = \emptyset$, cet ensemble est le même que

$$\{(L \vee K)\nu \mid \nu \in \Sigma_g, s\nu = t\nu\} \tag{3.2}$$

Quand $\bar{x} \cap \bar{y} = \emptyset$ on peut supposer que $Dom(\sigma) \cap Dom(\tau) = \emptyset$. Les ensembles (3.1) et (3.2) sont alors égaux parce que

— étant donnée σ et τ en (3.1), on peut définir ν en (3.2) par $\nu = \sigma \circ \tau$ $(= \tau \circ \sigma)$;

— étant donnée τ in (3.2), on peut définir en (3.2) $\sigma = \nu \mid_{\bar{x}}$ et $\tau = \nu \mid_{\bar{y}}$.

Par contre, cette égalité est en général fausse quand $\bar{x}$ et $\bar{y}$ ne sont pas disjoints. Par exemple, les termes x et $f(x)$ ont des instances communes (par exemple, $f(a)$), mais il n'y a aucune substitution ν telle que $x\nu = f(x)\nu$.

Si μ est un mgu de s et t, alors l'ensemble (3.2) est donc le même que

$$\{((L \vee K)\mu)\nu \mid \nu \in \Sigma_g\} \tag{3.3}$$

Le raisonnement pour la factorisation est analogue.

3.7.2 Résolution

On obtient donc les règles de résolution données sur la Figure 3.4. Dans les preuves par résolution, on n'écrit normalement pas les quantificateurs universels. Pourtant, il ne faut pas oublier que chaque clause est implicitement universellement quantifiée. Une conséquence importante est qu'on doit toujours assurer, avant d'appliquer un pas de résolution à deux clauses, que leur ensembles de variables soient disjoints. Si ce n'est pas le cas on est obligé de renommer les variables dans une des clauses. Finalement, si S est un ensemble de clauses du premier ordre, on note $S \vdash_{R1} C$ quand la clause C est obtenue à partir de S par une application des règles de la Figure 3.4.

Lemme 3.7.1 *Les règles de la résolution du premier ordre sont correctes : Si $S \vdash_{R1} C$ alors C est une conséquence logique de S.*

$$\text{Résolution binaire} \quad \frac{\forall \bar{x}(\neg P(\bar{s}) \vee L) \quad \forall \bar{y}(P(\bar{t}) \vee K)}{\forall \bar{z}((L \vee K)\sigma)} \quad \begin{array}{l} \sigma \text{ est un mgu de } \bar{s} \stackrel{?}{=} \bar{t} \\ \bar{x} = \mathrm{Var}(\neg P(\bar{s}) \vee L) \\ \bar{y} = \mathrm{Var}(P(\bar{t}) \vee K) \\ \bar{x} \cap \bar{y} = \emptyset \\ \bar{z} = \mathrm{Var}((L \vee K)\sigma) \end{array}$$

$$\text{Factorisation} \quad \frac{\forall \bar{x}(P(\bar{s}) \vee P(\bar{t}) \vee L)}{\forall \bar{z}((P(\bar{t}) \vee L)\sigma)} \quad \begin{array}{l} \sigma \text{ est un mgu de } \bar{s} \stackrel{?}{=} \bar{t} \\ \bar{x} = \mathrm{Var}(P(\bar{s}) \vee P(\bar{t}) \vee L) \\ \bar{z} = \mathrm{Var}((P(\bar{t}) \vee L)\sigma) \end{array}$$

FIGURE 3.4 – Règles de résolution pour la logique du premier ordre.

Lemme 3.7.2 *(Lemme de relèvement)*

- *Soient C_1 et C_2 des clauses, $D_1 \in H(C_1)$, $D_2 \in H(C_2)$, et $\{D_1, D_2\} \vdash_R D_3$ par résolution binaire. Alors il existe une clause C_3 telle que $\{C_1, C_2\} \vdash_{R1} C_3$ par résolution binaire et $D_3 \in H(C_3)$.*
- *Soit C_1 une clause, $D_1 \in H(C_1)$, et $\{D_1\} \vdash_R D_2$ par factorisation binaire. Alors il existe une clause C_2 telle que $\{C_1\} \vdash_{R1} C_2$ et $D_2 \in H(C_2)$.*

Preuve:
Soient

- $C_1 = \forall \bar{x}(P(\bar{s}) \vee L)$
- $C_2 = \forall \bar{y}(\neg P(\bar{t}) \vee K)$
- $\bar{x} \cap \bar{y} = \emptyset$
- $D_1 = (P(\bar{s}) \vee L)\sigma$
- $D_2 = (\neg P(\bar{t}) \vee K)\sigma$
- $\bar{s}\sigma = \bar{t}\sigma$

Résolution binaire sur $\{C_1, C_2\}$ nous donne une clause universelle $C_3 := \forall z(L \vee K)\mu$, où $\bar{z} \subseteq \bar{x} \cup \bar{y}$, et μ est un mgu de $\bar{s}$ et $\bar{t}$. Résolution binaire propositionnelle sur $\{D_1, D_2\}$ donne $D_3 := (L \vee K)\sigma$. Puisque σ est un unificateur de $\bar{s}$ et $\bar{t}$, et puisque μ est un mgu de $\bar{s}$ et $\bar{t}$, il y a une substitution ν telle que $\sigma = \nu \circ \mu$. Donc, $(L \vee K)\sigma = ((L \vee K)\mu)\nu$, donc $D_3 = (L \vee K)\sigma \in H(C_3)$.

La preuve pour la factorisation est analogue. □

Lemme 3.7.3 *Soit S un ensemble de clauses. Si $H(S) \vdash_R^* D$, alors il existe une clause C telle que $S \vdash_{R1}^* C$ et $D \in H(C)$.*

Preuve:
Par induction sur la structure de la preuve $H(S) \vdash_R^* D$:

- si $D \in H(S)$ alors il existe un $C \in S$ tel que $D \in H(C)$.
- si le dernier pas de la preuve de D est une résolution binaire $\{D_1, D_2\} \vdash_R D$: Par hypothèse de récurrence, il existe des clauses universelles closes C_1, C_2 telles que $S \vdash_{R1}^* C_1$, $S \vdash_{R1}^* C_2$, $D_1 \in H(C_1)$ et $D_2 \in H(C_2)$. Par

Lemme 3.7.2, il existe une clause universelle close C telle que $\{C_1, C_2\} \vdash_{R1} C$, donc $S \vdash^*_{R1} C$, et $D \in H(C)$.

— si le dernier pas de la preuve de D est une factorisation binaire : similaire. □

Théorème 3.7.1 *[Robinson] Soit S un ensemble de clauses (universelles, closes). S est insatisfaisable si et seulement si $S \vdash^*_{R1} \square$.*

Preuve:
Par Lemme 3.7.1, si $S \vdash^*_{R1} \square$ alors S n'est pas satisfaisable.

Soit S insatisfaisable. Par le théorème 3.4.4, $H(S)$ n'est pas satisfaisable. Donc, par la complétude de la résolution propositionnelle, $H(S) \vdash^*_R \square$. Il suit, par le lemme 3.7.3, que $S \vdash^*_{R1} \square$ (remarquez que, si $\square \in H(C)$ alors $C = \square$). □

Exemple 3.7.1 On considère l'ensemble des clauses

(1) $P(x, x)$
(2) $\neg P(x, y) \vee P(x, s(y)))$
(3) $\neg P(f(x), s(s(f(x))))$

On en déduit par résolution

(4) $P(x, s(x))$ résolution binaire sur (1), (2)
(5) $P(x, (s(s(x)))$ résolution binaire sur (4), (2)
(6) $\square$ résolution binaire sur (5), (3)

Exercice 122 (3)
Soit l'ensemble de clauses suivant :

(1) $\neg P(x) \vee Q(f(x), x)$
(2) $\neg P(x) \vee \neg Q(y, x) \vee R(y)$
(3) $\neg R(y) \vee \neg S(y) \vee \neg P(x) \vee \neg Q(y, x)$
(4) $\neg S(y) \vee R(y)$
(5) $P(a)$
(6) $\neg R(x) \vee S(x)$

En déduire par résolution $\square$.

Exercice 123 (5)
Soit S un ensemble fini de clauses, et qui possède un plus petit modèle de Herbrand $\mathcal{H}$. Montrer que $\mathcal{H}$ est récursivement énumérable, c'est-à-dire que $P_{\mathcal{H}}$ est récursivement énumérable pour tous les symboles de prédicat P.

La *stratégie négative* consiste à restreindre l'application d'une résolution binaire au cas où une des deux prémisses ne contient que des littéraux négatives (l'application de la factorisation n'est pas restreinte). On note $S \vdash^*_{R1\neg} C$ quand une clause C peut être obtenue à partir d'un ensemble de clauses S par résolution binaire en stratégie négative.

Théorème 3.7.2 *La résolution binaire restreinte à la stratégie négative est réfutationnellement complète : Un ensemble S de clauses universelles closes est non satisfaisable si et seulement si $S \vdash^*_{R1\neg} \square$.*

Preuve:
Dans le cas de la logique propositionnelle, la stratégie négative est réfutationnellement complète (c'est une exercice dans le chapitre sur la résolution dans la logique propositionnelle). Puisque S est non-satisfaisable, il y a une preuve $H(S) \vdash^*_{R\neg} \square$. Relèvement (comme dans la preuve du lemme 3.7.3) donne une preuve par résolution du premier ordre qui suit la stratégie négative. $\square$

Exercice 124
Montrer, qu'en général la preuve la plus courte par résolution négative est exponentiellement plus longue que la preuve la plus courte par résolution :

Donner une famille $(S_n)_{n\geq 1}$ d'ensembles finis de clauses universelles, telle que toute réfutation de S_n par résolution négative a la longueur $2^n + c_1$ pour une constante c_1, mais qu'il existe une réfutation de S_n par résolution de longueur $n + c_2$ pour une constante c_2.

Exercice 125 (6)
L'objet de l'exercice est de montrer un résultat général de complétude pour une famille de stratégies de résolution (inspiré de "Locked resolution").

$\mathcal{L}$ est un ensemble fini d'entiers, appelés étiquettes. Un *littéral étiqueté* est une paire d'un littéral et d'un élément de $\mathcal{L}$, noté L et e. Une *clause étiquetée* est une disjonction de littéraux étiquetés. Comme d'habitude, la disjonction vide est notée $\bot$. La sémantique d'une clause étiquetée est la même que celle de la clause à laquelle on a retiré les étiquettes. L'application d'une substitution σ à L et e est définie par $(L \text{ et } e)\sigma = L\sigma \text{ et } e$. Cette définition est étendue aux clauses.

Une *fonction de sélection* s est une application qui associe à toute clause étiquetée un sous-ensemble des littéraux de c.

Dans cette partie, on considère les deux règles d'inférence suivantes :

$$R \quad \frac{L \text{ et } e \vee C \quad \overline{L'} \text{ et } e' \vee C'}{(C \vee C')\sigma} \quad \texttt{Si} \begin{cases} \sigma = (L, L') \\ L \text{ et } e \in s(L \text{ et } e \vee C) \\ \overline{L'} \text{ et } e' \in s(\overline{L'} \text{ et } e' \vee C') \end{cases}$$

$$F \quad \frac{L \text{ et } e \vee L' \text{ et } e' \vee C}{(L \text{ et } e \vee C)\sigma} \quad \texttt{Si} \begin{cases} \sigma = (L, L') \\ L' \text{ et } e' \in s(L \text{ et } e \vee L' \text{ et } e' \vee C) \end{cases}$$

Soit C un ensemble de clauses. On affecte à chaque littéral de chaque clause de C une étiquette dans un ensemble fini (on peut affecter des étiquettes

différentes à un même littéral apparaissant dans deux clauses différentes). C est ainsi considéré comme un ensemble de clauses étiquetées.

Soit $\geq$ un ordre sur les littéraux clos (sans variable) étiquetés. *Dans toute la suite*, on considère la fonction de sélection suivante : $s(c)$ est l'ensemble des littéraux L et e tels qu'il existe une substitution σ telle que $(L \text{ et } e)\sigma$ est maximal dans $c\sigma$.

On note S_e cette stratégie (paramétrée par $\geq$ et l'étiquetage).

1. Dans cette question, on ne considère que des clauses closes (sans variable) et étiquetées et on suppose que $\geq$ est un ordre total bien fondé.

   À une clause $C = L_1 \text{ et } a_1 \vee \cdots \vee L_n \text{ et } a_n$ on associe le multi-ensemble des littéraux étiquetés $m(C) = \{L_1 \text{ et } a_1, \ldots, L_n \text{ et } a_n\}$. Les clauses sont ainsi ordonnées par l'extension multi-ensemble de $\geq$.

   Si $\mathcal{S}$ est un ensemble de clauses et L et a est un littéral étiqueté, on note $\mathcal{S}(L)$ l'ensemble des clauses C ne contenant aucun littéral L et b et telles que $C \in \mathcal{S}$ ou bien $C \vee \overline{L} \text{ et } b \in \mathcal{S}$ pour au moins un b. (Autrement dit, on remplace L par $\top$ dans les clauses de $\mathcal{S}$ et on simplifie).

   Si $\mathcal{E}$ est un ensemble de clauses, on note de plus $\mathcal{E}^*$ l'ensemble des clauses déductibles de $\mathcal{E}$ par la stratégie S_e.

   Montrer que, si $\bot \notin \mathcal{E}^*$, C est une clause minimale de $\mathcal{E}^*$ et L est un littéral maximal de C, alors $\bot \notin (\mathcal{E}^*(L))^*$.

   Montrer la complétude réfutationnelle de la stratégie S_e sur les clauses closes étiquetées.

2. Montrer que, pour tout ordre $\geq$ et tout étiquetage initial de l'ensemble de clauses, la stratégie S_e est réfutationnellement complète pour le calcul des prédicats en forme clausale.

3. Une clause (étiquetée) C *subsume* une clause (étiquetée) C', s'il existe une substitution σ et une clause C'' telles que $C' = C\sigma \vee C''$.

   Montrer que, si $\mathcal{E}$ est un ensemble de clauses étiquetées et $\mathcal{E}'$ un ensemble de clauses étiquetées telle que
   — pour toute clause $C \in \mathcal{E}$, il existe une clause $C' \in \mathcal{E}'$ qui subsume C
   — pour toute clause C déductible de $\mathcal{E}'$ par résolution et factorisaton, suivant la stratégie de sélection de la question 1.1, il existe une clause $C' \in \mathcal{E}'$ qui subsume C

   Alors, si $\mathcal{E}$ est insatisfaisable, $\mathcal{E}'$ contient la clause vide.

Chapitre 8

Théories décidables

8.1 Les théories du premier ordre

Les théories du premier ordre ont pour but de décrire une structure de données en l'axiomatisant. Le problème de la validité (qui est, comm déjà vu, récursivement énumérable et pas récursif, en logique du premier ordre) exprime en effet la validité d'un énoncé *dans toute structure*. Mais cela ne permet pas a priori d'exprimer des propriétés des listes ou des entiers ; il faut restreindre les structures d'interprétation. Les axiomes, des formules du premier ordre sans variable libre, expriment des propriétés de ces structures et permettent de se ramener au *Entscheidungsproblem* : si $\mathcal{A}$ "axiomatise" la structure $\mathcal{S}$, alors $\mathcal{S} \models \phi$ pourrait peu-être se ramener à $\mathcal{A} \models \phi$. Les structures $\mathcal{S}$ étant en général infinies, il n'y a pas beaucoup d'autre choix que de les décrire de cette manière. Tout cela doit être précisé et c'est ce que nous faisons ci-dessous.

On suppose donnés $\mathcal{F}, \mathcal{P}$ ensembles de symboles de fonction et de symboles de prédicat. On note Φ l'ensemble des formules du premier ordre sans variable libre, sur cet alphabet.

Definition 8.1.1 *Une* théorie *(du premier ordre) est un ensemble de formules $\mathcal{T} \subseteq \Phi$ telle que, pour tout $\phi \in |phi$, $\mathcal{T} \models \phi$ ssi $\phi \in \mathcal{T}$.*

Par exemple, si $\mathcal{S}$ est une structure du premier ordre, $\mathsf{Th}(\mathcal{S}) = \{\phi \in \Phi \,|\, \mathcal{S} \models \phi\}$ est une théorie. C'est la théorie de la structure $\mathcal{S}$.

Si $\mathcal{A} \subseteq \Phi$ est un ensemble récursif de formules, $\mathsf{Th}(\mathcal{A}) = \{\phi \in \Phi \mid \mathcal{A} \models \phi\}$ est une théorie. C'est la théorie axiomatisée par $\mathcal{A}$.

Nous nous intéresserons surtout à ce dernier type de théorie, les *théories axiomatiques*, et au problème de la déduction : est ce qu'une formule donnée est conséquence de $\mathcal{A}$? Autrement dit, est ce que cette formule est dans la théorie axiomatisée par $\mathcal{A}$?

Deux notions sont pertinentes pour mesurer l'adéquation d'une axiomatisation :

Definition 8.1.2 *Une théorie est $\mathcal{T}$ est* cohérente *si, pour tout $\phi \in \Phi$, $\phi \notin \mathcal{T}$ ou $\neg\phi \notin \mathcal{T}$.*

Une théorie est $\mathcal{T}$ est complète *si, pour tout $\phi \in \Phi$, $\phi \in \mathcal{T}$ ou $\neg\phi \in \mathcal{T}$.*

Deux modèles d'une théorie complète (et cohérente) sont *élémentairement équivalents* ; il satisfont les mêmes formules. Autrement dit, ils sont indistinguables par une formules du premier ordre. Le théorème de Löwenheim-Skolem entraine que, toute théorie cohérente et complète possède une infinité de modèles non isomorphes et élémentairement équivalents.

Remarquons que

— La théorie d'une structure est toujours cohérente et complète.

— Une théorie axiomatique complète est toujours récursive (car récursivement énumérable et co-récursivement énumérable).

Quelques exemples de théories :

complètes	récursives et incomplètes	indécidables
Ordres denses	Égalité	Arithmétique élémentaire
Arithmétique de Presburger	...	Arithmétique de Peano
Corps réels clos		Théorie des ensembles
Arbres finis		...

Dans ce chapitre, nous nous intéressons aux deux premières colonnes.

8.2 Élimination des quantificateurs

Nous nous limitons ici aux méthodes d'élimination des quantificateurs, basées sur les deux lemmes qui suivent.

Lemme 8.2.1 *Soit $\mathcal{A}$ un ensemble d'axiomes récursif. Si,*

1. *pour toute formule $\exists x.\phi$ où ϕ est sans quantificateur, on peut construire une formule ψ sans quantificateur telle que $\mathcal{A} \models \forall \vec{y}.((\exists x \phi) \leftrightarrow \psi)$*
2. *Pour toute formule sans variable Ω, on peut décider si $\mathcal{A} \models \Omega$ (resp. $\mathcal{A} \models \Omega$ ou $\mathcal{A} \models \neg\Omega$)*

alors $\mathsf{Th}(\mathcal{A})$ est récursive (resp. complète).

Preuve:

Si ϕ est une formule sans variable libre, sans perte de généralité, on peut supposer ϕ en forme prénexe : $\phi = Q_1 x_1, \ldots, Q_n x_n.\phi_0$ où ϕ_0 est sans quantificateur. On montre, par récurrence sur n que, sous les hypothèses de l'énoncé, on peut construire une formule ψ sans variable telle que $\mathcal{A} \models \phi \leftrightarrow \psi$.

Si $n = 0$, il suffit de choisir $\psi = \phi_0$.

Si $Q_n = \exists$, par hypothèse, on peut construire une formule ϕ_1 telle que $\mathcal{A} \models (\exists x_n.\phi_0) \leftrightarrow \phi_1$. Par hypothèse de récurrence, on peut construire ψ telle que $\mathcal{A} \models \psi \leftrightarrow Q_1 x_1, \ldots, Q_{n-1} x_{n-1}.\phi_1$ et ψ ne contient pas de variable. On a alors $\mathcal{A} \models \phi \leftrightarrow \psi$

Si $Q_n = \forall$, par hypothèse, on peut construire une formule ϕ_1 telle que $\mathcal{A} \models (\exists x_n.\neg\phi_0) \leftrightarrow \phi_1$, et donc $\mathcal{A} \models (\forall x_n, \phi_0) \leftrightarrow \neg\phi_1$. Par hypothèse de récurrence, on peut construire une formule ψ ne contenant pas de variable telle que $\mathcal{A} \models (Q_1 x_1 \ldots, Q_{n-1} x_{n-1} \neg\phi_1) \leftrightarrow \psi$. On a alors $\mathcal{A} \models \phi \leftrightarrow \psi$.

Pour décider si $\phi \in \mathsf{Th}(\mathcal{A})$ il suffit donc de construire la formule ψ sans variable équivalente et de décider si $\mathcal{A} \models \psi$.

Remarquons enfin que, si $\mathcal{A} \models \phi \leftrightarrow \psi$, alors $\mathcal{A} \models \neg\phi \leftrightarrow \neg\psi$. Donc, si pour toute formule sans variable ψ, $\mathcal{A} \models \psi$ ou $\mathcal{A} \models \neg\psi$, alors pour toute formule ϕ sans variable libre, $\mathcal{A} \models \phi$ ou $\mathcal{A} \models \neg\phi$.

Il n'est pas toujours possible d'éliminer directement un quantificateur. Dans ce cas, il peut être utile d'enrichir de manière conservative la théorie, en introduisant des symboles de prédicats correspondant aux formules dont on ne peut pas éliminer les quantificateurs :

Lemme 8.2.2 *Si $P \notin \mathcal{P}$ est un symbole de prédicat $n-aire$ et ϕ une formule du premier ordre sur $\mathcal{P}, \mathcal{F}$ à n variables libres*

$$\mathit{Th}(\mathcal{A}) = \mathit{Th}(\mathcal{A} \cup \{\forall x_1, \ldots, x_n.(P(x_1, \ldots, x_n) \leftrightarrow \phi(x_1, \ldots, x_n))\}) \cap \mathcal{F}_0(\mathcal{P})(\mathcal{F}, \mathcal{P})$$

Nous verrons un exemple plus loin d'utilisation de ces extensions.

8.3 La théorie des ordres denses

On considère les formules du premier ordre construites sur $\mathcal{F} = \emptyset$ et $\mathcal{P} = \{=, >\}$

La théorie des ordres denses est engendrée par les axiomes suivants :

Les axiomes de l'égalité (voir aussi section **??**) :

$$\begin{array}{lrcl}
\forall x. & & & x = x \\
\forall x, y. & x = y & \rightarrow & y = x \\
\forall x, y, z. & (x = y \wedge y = z) & \rightarrow & x = z \\
\forall x, y, z & (x = y \wedge x > z) & \rightarrow & y > z \\
\forall x, y, z & (x = y \wedge z > x) & \rightarrow & z > y
\end{array}$$

Ordre strict :

$$\begin{array}{lrcl}
\forall x. & & & \neg(x > x) \\
\forall x, y, z & (x < y \wedge y < z) & \rightarrow & x < z
\end{array}$$

Ordre total :

$$\forall x, y, \quad x > y \vee x = y \vee y > x$$

Ordre dense :

$$\forall x, y. \exists z. \quad (x > y \ \rightarrow \ (x > z \wedge z > y)$$

NoMin :

$$\forall x, \exists y. \quad x > y$$

NoMax :

$$\forall x, \exists y. \quad y > x$$

Théorème 8.3.1 *La théorie des ordres denses est décidable et complète.*

Preuve:
On s'appuie sur le lemme 8.2.1. On montre que, pour toute formule $\exists x.\phi$ où ϕ est sans quantificateurs, on peut effectivement calculer une formule ψ sans quantificateur telle que $\mathcal{O}_D \models (\exists x.\phi) \leftrightarrow \psi$.

Il suffit de considérer des formules ϕ en forme normale disjonctive, et donc des formules ϕ qui sont des conjonctions de formules atomiques. On peut supposer sans perte de généralité qu'aucune formule atomique n'est de la forme $x \neq y$: on les remplace par $x > y \vee y > x$ (puis remettre en FND). De même, on peut remplacer $x \not> y$ par $x = y \vee y > x$, $x > x$ par $\bot$ et $x = x$ par $\top$. Si ϕ contient $x = y$ (ou $y = x$), alors $\exists x.\phi \dashv\vdash \phi\{x \mapsto y\}$ et il suffit de choisir cette dernière formule pour ψ. Sinon, ϕ s'écrit $\bigwedge_{i\in I} x_i > x \wedge \bigwedge_{i\in J} x > x_i \wedge \phi'$, où ϕ' ne contient pas x.

- Si I est vide, $\exists x.\phi$ est équivalente 'a ϕ' (à cause de **NoMax**)
- Si J est vide, $\exists x.\phi$ est équivalente à ϕ' (à cause de **NoMin**)
- Si I, J sont non vides, alors, grâce à l'axiome de densité, et à la totalité,la formule est équivalente à $\phi' \wedge \bigwedge_{i\in I, j\in J} x_i > x_j$. En effet, si σ est une affectation qui satisfait cette formule, par totalité, $\min_{i\in I} x_i\sigma = x_{i_0}\sigma$ existe et $\max_{j\in J} x_j\sigma = x_{j_0}\sigma$ existe et de plus, $x_{i_0}\sigma >_{\mathcal{M}} x_{j_0}\sigma$. Par densité, il existe dans $\mathcal{M}$ un a tel que $x_{i_0}\sigma >_{\mathcal{M}} a >_{\mathcal{M}} x_{j_0}\sigma$. En étendant l'affectation σ en associant a à x, on obtient alors une affectation σ' telle que $\mathcal{M}, \sigma' \models \bigwedge_{i\in I} x_i > x \wedge \bigwedge_{i\in J} x > x_i \wedge \phi'$ et donc $\mathcal{M}, \sigma \models \exists x. \bigwedge_{i\in I} x_i > x \wedge \bigwedge_{i\in J} x > x_i \wedge \phi'$. Réciproquement, si $\mathcal{M}, \sigma \models \exists x. \bigwedge_{i\in I} x_i > x \wedge \bigwedge_{i\in J} x > x_i wedge\phi'$, par transitivité de l'ordre, $\mathcal{M}, \sigma \models \phi' \wedge \bigwedge_{i\in I, j\in J} x_i > x_j$.

Pour conclure, les seules formules sans variables sont les combinaisons booléenes de $\top, \bot$ et les hypothèses du lemme 8.2.1 sont donc satisfaites : la théorie est complète et décidable.

Exercice 198
Montrer que, si l'on remplace **NoMin** (resp. **NoMax**) par sa négation, on obtient à nouveau une théorie décidable et complète. En donner deux modèles non isomorphes.

Exercice 199
Montrer que, si l'on retire **NoMin** (resp. **NoMax**), la théorie engendrée reste décidable, mais est incomplète.

La procédure, telle qu'elle est décrite, est, a priori, non-élémentaire, puisque, pour chaque élimination de quantificateur, la formule sans quantificateur est mise en forme normale disjonctive, ce qui conduit a priori a une complexité exponentielle pour chacune de ces étapes. (La complexité est a priori une tour d'exponentielles dont la hauteur est proportionnelle au nombre de variables). Cependant, pour décider si ϕ est dans la théorie, la complétude de la théorie permet de se ramener au problème de savoir si $\mathbb{Q} \models \phi$, ce qu'on peut faire de manière plus efficace, comme le montre l'exercice suivant.

Exercice 200
1. Soit ϕ une formule de variables libres $x_1, \ldots, x_n$ et $\sigma_1 = \{x_1 \mapsto a_1, \ldots, x_n \mapsto a_n\}$, $\sigma_2 = \{x_1 \mapsto b_1, \ldots, x_n \mapsto b_n\}$ deux affectations à valeurs dans $\mathbb{Q}$

telles que $a_1 < \ldots < a_n$ et $b_1 < \ldots < b_n$. Montrer que $\mathbb{Q}, \sigma_1 \models \phi$ ssi $\mathbb{Q}, \sigma_2 \models \phi$.

2. Si $a_1 \leq \cdots \leq a_n$ (dans $\mathbb{Q}$), et σ est une affectation $x_{i_1} \mapsto a_1, \ldots, x_{i_n} \mapsto a_n$ des variables libres $x_1, ..., x_n$ de $\forall x.\phi$, montrer que $\sigma \models \forall x.\phi$ ssi
   — ou bien $n = 0$ et $\{x \mapsto 0\} \models \phi$
   — ou bien $n > 0$ et toutes les propriétés suivantes sont satisfaites :
      — pour tout $i = 1, \ldots, n$, $\sigma, \{x \mapsto a_i\} \models \phi$
      — $\sigma, \{x \mapsto a_1 - 1\} \models \phi$
      — $\sigma, \{x \mapsto a_n + 1\} \models \phi$
      — pour tout $i = 1, \ldots, n-1$, $\sigma, x \mapsto \frac{a_i + a_{i+1}}{2} \models \phi$.
3. Donner un équivalent de la question précédente lorsque la formule est existentielle.
4. Montrer que la théorie des ordres denses est dans PSPACE
5. Montrer que la théorie des ordres denses est PSPACE-complète.

8.4 La théorie de l'égalité

La théorie engendrée par les seuls axiomes de l'égalité est incomplète puisque

$$\mathcal{A}_{eq} \not\models \forall x, y.x = y \qquad \mathcal{A}_{eq} \not\models \exists x, y, x \neq y$$

Il existe en effet des modèles à un élément et des modèles à plus de un élément.

Nous utilisons alors une extension conservative. Soit, pour $n \in \mathbb{N}$ la formule :

$$E_n \quad \stackrel{\text{def}}{=} \quad \exists x_1, \ldots, x_n. \bigwedge_{i=1}^{n-1} \bigwedge_{j=i+1}^{n} x_i \neq x_j$$

Par convention, $E_0 = \top$.

Lemme 8.4.1 *$\mathcal{M} \models E_n$ ssi $|\mathcal{M}|$ a au moins n classes d'équivalence modulo l'interprétation de $=$.*

Preuve:
En effet, si $\mathcal{M} \models E_n$, alors il existe une affectation σ de $x_1, \ldots, x_n$ telle que $x_i\sigma =_{\mathcal{M}} x_j\sigma$ ssi $i = j$. $|\mathcal{M}$ contient alors au moins $x_1\sigma, \ldots, x_n\sigma$, qui sont non équivalents deux à deux. Réciproquement, si $|\mathcal{M}|$ contient n éléments $a_1, \ldots, a_n$ qui sont non-équivalents deux à deux, il suffit de choisir une affectation σ telle que $x_i\sigma = a_i$: $\mathcal{M}.\sigma \models \bigwedge_{i=1}^{n-1} \bigwedge_{j=i+1}^{n} x_i \neq x_j$.

On utilise alors la théorie $\mathcal{A}_{eq}^{+}$ en ajoutant les variables proprositionnelles E_i au langage et les axiomes

$$E_n \leftrightarrow \exists x_1, \ldots, x_n. \bigwedge_{i=1}^{n-1} \bigwedge_{j=i+1}^{n} x_i \neq x_j$$

Cette axiomatisation n'est pas finie, mais reste récursive.

Théorème 8.4.1 *La théorie engendrée par $\mathcal{A}^+_{eq}$ est récursive.*

Preuve:
Nous nous appuyons à nouveau sur le lemme 8.2.1.

Si $\phi = \exists x.\phi_0$ où ϕ_0 est sans quantificateurs, on peut supposer sans perte de généralité que ϕ_0 est en forme normale disjonctive et il suffit de montrer comment éliminer le quantificateur existentiel lorsque ϕ_0 est une conjonction de formules atomiques. On remplace aussi $x \neq x$ par $\bot$ et $x = x$ par $\top$ et on simplifie la formule.

Si ϕ_0 est de la forme $x = y \wedge \phi_1$ (ou $y = x \wedge \phi_1$), avec y distinct de x, il suffit de remplacer x par y dans ϕ_1 pour obtenir une formule ψ telle que $\mathcal{A}^+_{eq} \models (\phi \leftrightarrow \psi)$ (et ψ ne contient pas x).

Sinon, ϕ_0 s'écrit $x \neq x_1 \wedge \ldots \wedge x \neq x_n \wedge \phi'$ où ϕ' ne contient pas x. On note alors $\mathcal{E}(x_1, \ldots, x_n)$ l'ensemble des relationss d'équivalence sur l'ensemble $\{x_1, \ldots, x_n\}$. Si R est une telle relation d'équivalence, on note encore n_R le cardinal du quotient par R. On montre alors que

$$\mathcal{A}^+_{eq} \models \exists x.x \neq x_1 \wedge \ldots \wedge x \neq x_n \leftrightarrow \bigvee_{R \in \mathcal{E}(x_1,\ldots,x_n)} (E_{n_R+1} \wedge \bigwedge_{(x_i,x_j)\in R} x_i = x_j)$$

Si $\mathcal{M}$ est une structure et σ est une affectation de $x_1, \ldots, x_n$ dans $|\mathcal{M}|$ et $\mathcal{M}, \sigma \models \exists x.x \neq x_1 \wedge \ldots \wedge x \neq x_n$ alors il existe $a \in |\mathcal{M}|$, $a \neq_{\mathcal{M}} x_1\sigma, \ldots a \neq_{\mathcal{M}} x_n\sigma$. Donc, si R est la relation telle que $x_i R x_j$ ssi $x_i\sigma =_{\mathcal{M}} x_j\sigma$, $\mathcal{M}, \sigma \models E_{n_R+1} \wedge \bigwedge_{(x_i,x_j)\in R} x_i = x_j$.

Réciproquement, si, pour une relation R sur $\{x_1, \ldots, x_n\}$, $\mathcal{M}, \sigma \models E_{n_R+1} \wedge \bigwedge_{(x_i,x_j)\in R} x_i = x_j$, alors $|\mathcal{M}|$ contient au moins $n_R + 1$ classes d'équivalence, en particulier, il existe $a \in |\mathcal{M}|$ tel que $a \neq_{\mathcal{M}} x_1\sigma, \ldots a \neq_{\mathcal{M}} x_n\sigma$. Donc $\mathcal{M}, \sigma \models \exists x.x \neq x_1 \wedge \ldots \wedge x \neq x_n$.

Nons avons donc montré la première condition du lemme 8.2.1.

Les formules sans variables de cette théorie sont des combinaisons Booléennes de variables propositionnelles E_i. Soit ψ une telle formule. et N l'indice maximal d'une variable propositionnelle E_i apparaissant dans ψ. Nous montrons que

$$\mathcal{A}^+_{eq} \models \psi \qquad \text{ssi} \qquad \{E_{i+1} \to E_i \mid i < N\} \models \psi$$

Si $\{E_{i+1} \to E_i \mid i < N\} \models \psi$, comme $\mathcal{A}^+_{eq} \models E_{i+1} \to E_i$ pour tout i, $\mathcal{A}^+_{eq} \models \psi$.

Réciproquement, si I est une interprétation des variables propositionnelles $E_0, \ldots, E_n$ qui falsifie $(\bigwedge_{i=1}^N E_{i+1} \to E_i) \to \psi$, alors $I = \{E_0, \ldots, E_k\}$. Si $\mathcal{M}$ est une structure dans laquelle le nombre de classes d'équivalence modulo $=_{\mathcal{M}}$ est exactement k, $\mathcal{M} \models E_0 \wedge \ldots \wedge E_k$ et $\mathcal{M} \not\models E_{k+1} \vee \ldots \vee E_n$. Il s'en suit (comme I falsifie ψ et par récurrence sur la formule propositionnelle) que $\mathcal{M} \not\models \psi$.

Pour décider si une formule ψ sans variable est une conséquence de la théorie, il suffit donc de décider de la validité de la formule propositionnelle $(\bigwedge_{i=1}^N E_{i+1} \to E_i) \to \psi$, ce qui peut se faire en temps exponentiel.

Par le lemme 8.2.1 $\mathsf{Th}(\mathcal{A}^+_{eq})$ est donc récursive.

D'après le lemme 8.2.2, on obtient alors :

Corollaire 8.4.1 *$Th(\mathcal{A}_{eq})$ est récursive.*

À nouveau, la méthode d'élimination de quantificateurs ne donne, a priori, qu'une borne de complexité non-élémentaire à la théorie. Mais on peut faire mieux, en utilisant une propriété de petit modèle ;

Exercice 201

1. Soit ϕ une formule close en forme prénexe dont le nombre de variables est n. Montrer que $\mathcal{A}_{eq} \models \phi$ si et seulement si, pour tout modèle $\mathcal{M}$ de cardinal au plus $n+1$, $\mathcal{M} \models \phi$..
2. En déduire que la théorie engendrée par les axiomes de l'égalité est PSPACE-complet.

8.5 Autres exemples de théories décidables/complètes

8.5.1 La théorie des ordres discrets

Cette théorie (Sur $\mathcal{P} = \{=, \geq\}, \mathcal{F} = \emptyset$) est axiomatisée par les axiomes de l'égalité et les axiomes :

$(TO1)$ $\forall x.x \geq x$
$(TO2)$ $\forall x, y.(x \geq y \wedge y \geq x) \rightarrow x = y$
$(TO3)$ $\forall x, y, z.(x \geq y \wedge y \geq z) \rightarrow x \geq z$
$(TO4)$ $\forall x, y.(x \geq y \vee y \geq x)$
(1) $\exists x.\forall y.y \geq x$
(2) $\forall x.\exists y.y \geq x \wedge y \neq x \wedge (\forall z.(z \geq x \wedge z \neq y \rightarrow z \geq y))$
(3) $\forall x.(\forall y.y \geq x) \vee (\exists z.z \leq x \wedge z \neq x \wedge (\forall y.y \geq z \rightarrow (y = z \vee y \geq x)))$

On étend la théorie en introduisant deux symboles de fonction 0 et s et les axiomes :

$$(D_1) \quad \forall x. \quad x = 0 \leftrightarrow \forall y.y \geq x$$

$$(D_2) \quad \forall x, y. \quad x = s(y) \leftrightarrow (y \geq x \wedge y \neq x \wedge \forall z.z \geq x \rightarrow (z = x \vee z \geq y))$$

Exercice 202

1. Montrer qu'on peut dériver les axiomes suivants :

$$\begin{array}{cccc} \forall x. & & & x \geq 0 \\ \forall x.x \neq 0 & \rightarrow & \exists y.x = s(y) & \\ \forall x. & & & 0 \neq s(x) \\ \forall x, y. \quad s(x) = s(y) & & \rightarrow & x = y \end{array}$$

2. Montrer qu'il s'agit d'une extension conservative :

$$\mathsf{Th}(TOD) = \mathsf{Th}(TOD \cup \{D_1, D_2\}) \cap FO(\{\geq, =\}, \emptyset)$$

3. Montrer que la théorie des ordres discrets est complète et récursive.

Exercice 203
Montrer que TOD a des modèles dans lesquels l'ordre n'est pas bien fondé ; en déduire qu'on ne peut pas axiomatiser au premier ordre la bonne fondaison de l'ordre.

Exercice 204
Montrer que (TO_4) n'est pas une conséquence des autres axiomes de TOD

Chapitre 9

Théories indécidables

9.1 Exemples de théories de l'arithmétique

Arithmétique élémentaire Dans les deux exemples suivant, $\mathcal{F}$ contient $\{0(0), s(1), +(2), \times(2)\}$ et $\mathcal{P} = \{=\}$.

On considère maintenant l'*arithmétique élémentaire* Q engendrée par les formules de la figure 9.1 et les axiomes de l'égalité.

Nous verrons que Q n'est pas complète et n'est pas récursive.

Exercice 211
Montrer que $Q \not\models \forall x.x \neq s(x)$.

Exercice 212
Donner un modèle de Q dans lequel l'addition n'est pas commutative.

Arithmétique de Peano L'*arithmétique de Peano* est la théorie PA, engendrée par les axioms de la figure 9.1, les axiomes de l'égalité ainsi que l'ensemble (récursif) d'axiomes :e

$$(\phi(0) \wedge (\forall x.\phi(x) \rightarrow \phi(s(x)))) \rightarrow \forall x.\phi(x)$$

où ϕ est une formule du premier ordre arbitraire avec une variable libre.

$$\begin{array}{lll}
(A_1) & \forall x. & s(x) \neq 0 \\
(A_2) & \forall x, y. & s(x) = s(y) \Rightarrow x = y \\
(A_3) & \forall x. & x + 0 = x \\
(A_4) & \forall x, y. & x + s(y) = s(x + y) \\
(A_5) & \forall x. & x \times 0 = 0 \\
(A_6) & \forall x, y. & x \times s(y) = (x \times y) + x \\
(A_7) & \forall x. & x \neq 0 \Rightarrow \exists y.x = s(y)
\end{array}$$

FIGURE 9.1 – Axiomes de l'arithmétique élémentaire

Exercice 213
Expliquer pourquoi l'axiomatisation de PA est récursive.

Exercice 214
Montrer que $PA \vdash \forall x, y.\ x + y = y + x$

D'autres exemples de théories seront donnés dans le chapitre 8.

9.2 Codages des formules

On suppose donnés un ensemble dénombrable de symboles de fonction avec leur arité (on notera $f[n]m$ la $m$ième fonction d'arité n, m et n étant des mots de $\{0,1\}^*$ représentant des entiers en binaires), un nombre dénombrable de symboles de prédicats avec leur arité (on notera $P[n]m$ ces symboles de prédicat) et un nombre dénombrable de variables (vn).

Les formules du premier ordre sur cet alphabet sont alors des mots sur l'alphabet $\{0, 1, p, f, v, \vee, \wedge, \rightarrow, \neg, "[", "]", "(", ")", ",", ""\{", "\}"\}$. Ils peuvent être considèrés comme des entiers écrits dans une base appropriée. On note $< \phi >$ l'entier associé à ϕ. Noter que $< \phi >=< \psi >$ entraine $\phi = \psi$. Dans la suite on parlera d'ensemble de termes ou de formules récursifs en faisant référence à leur codage dans les entiers.

Par ailleurs, on supposera que les entiers peuvent être représentés dans la logique : pour tout $n \in \mathbb{N}$, soit $\overline{n}$ le terme qui représente n. On suppose ce codage récursif : $n \mapsto < \overline{n} >$ est une fonction récursive.

On obtient, via par exemple l'équivalence avec les machines de Turing (théorème 7.3.1), les résultats de récursivité :

Lemme 9.2.1 *Les fonctions/ensembles suivants sont récursifs :*
- $\{< \phi > \mid \phi \in CP_1(\mathcal{P}, \mathcal{F}, \mathcal{X})\}$
- *Le sous-ensemble du précédent des formules ayant exactement une variable libre.*
- *La fonction qui à $n, < \phi >$ associe $\phi\{x \mapsto \overline{n}\}$ si ϕ est une formule avec exactement une variable libre x et $\overline{0}$ sinon.*

9.3 Fonctions représentables

Definition 9.3.1 *Une fonction partielle f sur les entiers est* représentable *dans une théorie T s'il existe une formule ϕ_f telle que, pour tous entiers $n_1, \ldots, n_k$ et tout entier m,*

1. *$f(n_1, \ldots, n_k) = m$ entraine $T \models \phi_f(\overline{n_1}, \ldots, \overline{n_k}, \overline{m})$*
2. *$f(n_1, \ldots, n_k) \neq m$ (ou bien $f(n_1, \ldots, n_k)$ est indéfinie) entraine $T \models \neg\phi_f(\overline{n_1}, \ldots, \overline{n_k}, \overline{m})$.*
3. *$f(\vec{n}) = m$ entraine $T \models \forall x.\phi_f(\overline{n_1}, \ldots, \overline{n_k}, x) \rightarrow x = \overline{m}$.*