3.6 Unification

Nous avons ramené la satisafaisabilité d'une formule (ou d'un ensemble de formules) du premier ordre à la satisfaisabilité d'un ensemble de clauses (paragraphe 3.4). Puis, grâce au théorème de Herbrand (théorème 3.5.1), un ensemble de clauses est satisfaisable si et seulement si il a un modèle de Herbrand. Et donc, un ensemble de clauses est satisfaisable si et seulement si l'ensemble de ses instances closes est satisfaisable, chaque littéral clos étant vu comme une variable propositionnelle. Nous nous sommes ainsi ramenés à la satisfaisabilité en calcul propositionnel. Cependant, l'ensemble de formules (et de variables proporitionnel) est a priori infini. Il nous faut donc maintenant un moyen effectif de manipuler des ensembles infinis de clauses qui sont les instances closes d'un ensemble de clauses avec variables.

Ceci nous amène à étudier la représentation suivante d'ensembles infinis de termes : si $t \in T(\mathcal{F}, \mathcal{X})$, on note $[\![t]\!]$ l'ensemble des termes de $T(\mathcal{F})$ qui sont des instances de t :

$$[\![t]\!] \stackrel{\text{def}}{=} \{t\sigma \in T(\mathcal{F}) \mid \sigma \in \Sigma\}$$

où Σ est l'ensemble des morphismes de $T(\mathcal{F}, \mathcal{X})$ dans $T(\mathcal{F})$ (substitutions closes).

L'ensemble des termes $T(\mathcal{F}, \mathcal{X})$ (ou plutôt l'ensemble des termes à similarité près)est ainsi muni d'une structure de semi-treillis : $t \leq u$ si $[\![u]\!] \subseteq [\![t]\!]$ (lire "t est plus général que u"). Le treillis possède un élément minimal et le sup de deux éléments est calculable : $[\![t]\!] \cap [\![u]\!]$ est un ensemble obtenu par *unification de t et u*. C'est cette propriété fondamentale que nous utiliserons pour *relever* résolution et factorisation au premier ordre.

Nous rappelons que pour une substitution σ, son *domaine* est défini comme $Dom(\sigma) := \{x \mid \sigma(x) \neq x\}$.

La substitution obtenue par l'application d'abord de σ puis de τ est notée $\sigma\tau$. Dans cette notation, on a donc que $t(\sigma\tau) = (t\sigma)\tau$ pour tout terme t et toutes substitutions σ et τ.

Une substitution σ est *idempotente* si $\sigma = \sigma\sigma$.

Definition 3.6.1 *Un* problème d'unification *est soit $\perp$, soit une conjonction d'équations $s_1 \stackrel{?}{=} t_1 \wedge \ldots \wedge s_n \stackrel{?}{=} t_n$ avec $s_i, t_i \in T(\mathcal{F}, \mathcal{X})$. (Par convention, on note $\top$ ce problème lorsque $n = 0$).*

Une substitution σ est une solution *(aussi appelée* unificateur*) d'un problème d'unification $s_1 \stackrel{?}{=} t_1 \wedge \ldots \wedge s_n \stackrel{?}{=} t_n$ si, pour tout i, $s_i\sigma = t_i\sigma$.*

Une substitution μ est un unificateur le plus général *(angl. : most general unifier), abrégé* mgu*, d'un problème d'unification $P = (s_1 \stackrel{?}{=} t_1 \wedge \ldots \wedge s_n \stackrel{?}{=} t_n)$ si*

1. *μ est un unificateur de P ;*
2. *μ est idempotent ;*
3. *pour chaque unificateur τ de P il existe une substitution ν telle que $\tau = \mu\nu$*

Attention, il existe dans la littérature des définitions d'un mgu qui sont légèrement différentes mais équivalentes à la notre, mais aussi des définitions légèrement différentes et pas équivalentes à la notre. En l'occurrence, on trouve aussi une définition qui n'exige pas que le mgu soit idempotent.

Proposition 3.6.1 *Une substitution σ est idempotente ssi $Dom(\sigma) \cap VIm(\sigma) = \emptyset$.*

<u>Preuve:</u>
Soit $y \in Dom(\sigma) \cap VIm(\sigma)$. Il existe alors $x \in Dom(\sigma)$ tel que $y \in Var(x\sigma)$. Puisque $y\sigma \neq y$, on obtient alors que $x\sigma\sigma \neq x\sigma$, donc σ n'est pas idempotent.

Soit $Dom(\sigma) \cap VIm(\sigma) = \emptyset$. Si $x \notin Dom(\sigma)$ alors $x\sigma = x$ et donc $x\sigma\sigma = x$. Si $x \in Dom(\sigma)$, alors $x\sigma\sigma = x\sigma$ puisque $Dom(\sigma) \cap Var(x\sigma) = \emptyset$. □

Exemple 3.6.1

1. Le problème d'unification $x \stackrel{?}{=} g(y, z) \wedge f(x) \stackrel{?}{=} f(a)$ n'a pas d'unificateur.
2. Le problème d'unification $x \stackrel{?}{=} f(x)$ n'a pas d'unificateur.
3. Soit le problème d'unification $f(x) \stackrel{?}{=} f(g(y))$. Les substitutions suivantes sont des unificateurs :

$$\begin{aligned} \sigma_1 = &\quad \{x \to g(y)\} \\ \sigma_2 = &\quad \{x \to g(a); y \to a\} \end{aligned}$$

   σ_1 est un mgu, σ_2 ne l'est pas. En fait, $\sigma_2 = \sigma_1 \circ \{y \to a\}$, mais il n'y a aucune substitution ν telle que $\sigma_1 = \sigma_2 \circ \nu$.
4. Soit le problème d'unification

$$f(x, x) \stackrel{?}{=} f(x, y) \wedge g(x) \stackrel{?}{=} g(g(z)) \wedge f(z, a) \stackrel{?}{=} f(z', a)$$

   Les substitutions suivantes sont toutes des mgu :

$$\begin{aligned} &\{x \to g(z'); y \to g(z'); z \to z'\} \\ &\{x \to g(z); y \to g(z); z' \to z\} \end{aligned}$$

5. Soit le problème d'unification $g(x) \stackrel{?}{=} g(g(z)) \wedge f(a, z) \stackrel{?}{=} f(a, y)$. Les substitutions suivantes sont des unificateurs :

$$\begin{aligned} \sigma_1 = &\quad \{x \to g(z); y \to z\} \\ \sigma_2 = &\quad \{x \to g(w); y \to w; z \to w; w \to y\} \end{aligned}$$

   σ_1 est un mgu, en fait $\sigma_2 = \sigma_1 \circ \{z \to w, w \to y\}$. On aussi que $\sigma_1 = \sigma_2 \circ \{w \to z; y \to w\}$, mais σ_2 n'est pas idempotent (parce que $w \in Dom(\sigma_2) \cap VIm(\sigma_2)$) donc pas un mgu.

Exercice 89 (4)
Soit μ un mgu d'un problème d'unification P. Montrer que, pour toute substitution σ :

$$\sigma \text{ est un unificateur de } P \quad \Leftrightarrow \quad \sigma = \mu\sigma$$

Exercice 90
Montrer que le mgu est unique à renommage près :

Soient μ et ν deux mgus d'un problème d'unification P. Montrer qu'il y a un *renommage* ρ tel que $\mu = \nu\rho$.

Un système de règles pour les problèmes d'unification est donné dans la Figure 3.3. Dans ces règles, ont suppose que le symbole $\wedge$ est associatif et commutatif. De plus, on suppose que le symbole d'égalité est commutatif, c'est-à-dire on identifie $s \stackrel{?}{=} t$ avec $t \stackrel{?}{=} s$. On note $P \rightarrow_U P'$ quand on peut transformer par une des règles de la Figure 3.3 un problème d'unification P dans un problème d'unification P'.

Proposition 3.6.2 *Les règles de la Figure 3.3 sont correctes : Si $P \rightarrow_U P'$ alors P et P' ont les mêmes unificateurs.*

On dit qu'une variable x est *résolue* dans un problème d'unification P quand P est de la forme $x \stackrel{?}{=} t \wedge P'$, $x \notin \mathrm{Var}(t)$ et $x \notin \mathrm{Var}(P')$.

Proposition 3.6.3 *Les règles de la Figure 3.3 terminent : Il n'y a pas de séquence infinie $P_1 \rightarrow_U \ldots \rightarrow_U P_n \rightarrow_U \ldots$*

Avant de commencer la preuve, rappelons les définitions des extensions lexicographique et multi-ensemble.

Si $E_1, \ldots, E_n$ sont des ensembles ordonnés par $\geq_1, \ldots, \geq_n$, la *composée lexicographique* de $\geq_1, \ldots, \geq_n$ est la relation d'ordre définie sur $E_1 \times \ldots \times E_n$ par :

$$(a_1, \ldots, a_n) >_{lex} (b_1, \ldots, b_n) \;\text{ ssi }\; \exists i. a_1 = b_1, ..., a_{i-1} = b_{i-1}, a_i >_i b_i$$

Un ordre est *bien fondé* s'il n'y a pas de suite infinite strictement décroissante.

Exercice 91
Montrer que la composée lexicographique de $\geq_1, \ldots, \geq_n$ est bien fondée si et seulement si chacun des ordres $\geq_1, \ldots, \geq_n$ est bien fondé.

Un *multi-ensemble (fini)* sur E est une application de E dans $\mathbb{N}$, qui est nulle sauf pour un nombre fini d'éléments de E. On note en outre $M_1 + M_2$ l'application $(M_1 + M_2)(x) \stackrel{\text{def}}{=} M_1(x) + M_2(x)$, $\emptyset$ l'application nulle, $x \in M$ si $M(x) \geq 1$ et enfin $M \setminus N$ l'application $(M \setminus N)(x) \stackrel{\text{def}}{=} \max(M(x) - N(x), 0)$. On note $\{\underbrace{x_1, \ldots x_1}_{n_1}, \ldots, \underbrace{x_k, \ldots, x_k}_{n_k}\}$ le multi-ensemble M tel que $M(x_1) = n_1, \ldots, M(x_k) = n_k$.

Si E est un ensemble ordonné par $\geq$, l'*extension multi-ensemble* de $\geq$ est la relation $\geq_m$ est la plus petite relation transitive telle que :

1. pour tout M, $M \geq_m \emptyset$

Decompose	$\phi \wedge f(s_1, \ldots, s_n) \stackrel{?}{=} f(t_1, \ldots, t_n) \rightarrow_U \phi \wedge s_1 \stackrel{?}{=} t_1 \wedge \ldots \wedge s_n \stackrel{?}{=} t_n$
Clash	$\phi \wedge f(s_1, \ldots, s_n) \stackrel{?}{=} g(t_1, \ldots, t_m) \rightarrow_U \bot$ si $f \neq g$
Trivial	$\phi \wedge s \stackrel{?}{=} s \rightarrow_U \phi$
Replace	$\phi \wedge x \stackrel{?}{=} t \rightarrow_U \phi[x \mapsto t] \wedge x \stackrel{?}{=} t$ si $x \in \mathrm{Var}(\phi)$, $t \notin \mathcal{X}$ et $x \notin \mathrm{Var}(t)$
Occur Check	$\phi \wedge x \stackrel{?}{=} t \rightarrow_U \bot$ si $x \in \mathrm{Var}(t)$ et $t \notin \mathcal{X}$
Var Replace	$\phi \wedge x \stackrel{?}{=} y \rightarrow_U \phi\{x \mapsto y\} \wedge x \stackrel{?}{=} y$ Si $x \in \mathrm{Var}(\phi)$, $x \neq y$ et $y \in \mathrm{Var}(\phi)$
General OC	$\phi \wedge x_1 \stackrel{?}{=} t_1[x_2]_{p_1} \wedge \ldots \wedge x_n = t_n[x_1]_{p_n} \rightarrow_U \bot$ si au moins l'un des p_i est non vide
Fusion	$\phi \wedge x = s \wedge x = t \rightarrow_U \phi \wedge x = s \wedge s = t$ si $s \notin \mathcal{X}$ et $\lvert s\rvert \leq \lvert t\rvert$

Fig. 3.3 – Règles d'unification.

2. si $M \geq_m M'$, alors $M + N \geq_m M' + N$
3. si $\forall y \in N$, $x > y$ et $M \geq_m M'$, alors $M + \{x\} >_m M' + N$

Exercice 92
Montrer que $\geq_m$ est antisymétrique et réflexive.

Exercice 93
Montrer que $M \geq_m M'$ si et seulement si, il existe N, M_1, M'_1 tels que
- $M = M_1 + N$ et $M' = M'_1 + N$
- $\forall x \in M'_1, \exists y \in M_1,\ y > x$

Exercice 94
Montrer que $\geq$ est bien fondée si et seulement si $\geq_m$ est bien fondée.

Revenons à la preuve du lemme de terminaison :

Preuve:
On considère les fonctions d'interprétation suivantes des problèmes d'unification :
- $\phi_1(P)$ est le nombre de variables non résolues de P.
- Si $P \equiv s_1 = t_1 \wedge \ldots \wedge s_n = t_n$, alors $\phi_2(P)$ est le multi-ensemble $\{m_1, \ldots, m_n\}$ où $m_i = \max(|s_i|, |t_i|)$.
- $\phi_3(P)$ est le nombre d'équations de P dont l'un des membres au moins est une variable.

$\phi(P)$ est le triplet $(\phi_1(P), \phi_2(P), \phi_3(P))$. L'ensemble de ces triplets est muni de la composée lexicographique de trois ordres :

1. L'ordre habituel sur les entiers naturels
2. L'extension multi-ensemble de l'ordre sur les entiers naturels
3. L'ordre habituel sur les entiers naturels

Il est ainsi muni d'un ordre bien fondé puisque construit à partir d'extensions multi-ensemble et lexicographiques d'ordres bien fondés.

Il suffit maintenant de montrer que si $P \rightarrow_U Q$ alors $\phi(P) > \phi(Q)$. Le sens de variations des trois fonctions d'interprétation est résumé dans le tableau ci-dessous :

	ϕ_1	ϕ_2	ϕ_3
Trivial	$\preceq$	$\prec$	
Decompose	$\preceq$	$\prec$	
Clash	$\preceq$	$\prec$	
Replace	$\prec$		
Var replace	$\prec$		
Fusion	$\preceq$	$=$	$\prec$
Occur check	$\preceq$	$\prec$	
General OC	$\preceq$	$\prec$	

Il n'est pas difficile de vérifier qu'aucune règle ne crée de nouvelle variable non-résolue. Les conditions d'application des deux règles d'élimination et de remplacement de variables garantissent par ailleurs qu'une variable non résolue

(x dans la formulation des règles doit apparaitre dans P) devient résolue après leur application.

Notons également que la règle de décomposition fait bien décroître ϕ_2 puisqu'elle remplace $m = \max(|f(s_1, \ldots, s_n)|, |f(t_1, \ldots, t_n)|)$ par n entiers strictement inférieurs.

La règle de fusion conserve bien ϕ_2 à cause de la condition $|s| \leq |t|$: $\max(|x|, |t|) = \max(|s|, |t|)$. Enfin, ϕ_3 est bien décroissante par fusion à cause de la condition $s \notin x$ qui, avec $|s| \leq |t|$, garantit que $s = t$ est une équation dont aucun des membres n'est une variable.

Bien entendu certaines fonctions d'interprétation (ϕ_2 ou ϕ_3) peuvent croître par application de certaines règles, mais la composée lexicographique des trois interprétations est toujours décroissante comme le montre le tableau ci-dessus.

$\square$

Definition 3.6.2 *Un problème d'unification est en* arbre-forme résolue *si c'est* $\bot$, $\top$ *ou bien* $x_1 \stackrel{?}{=} t_1 \wedge \ldots \wedge x_n \stackrel{?}{=} t_n$ *où* $x_1, \ldots, x_n$ *sont des variables et n'apparaissent qu'une seule fois dans le problème.*

Exercice 95
Montrer qu'un problème d'unification en arbre-forme résolue comme ci-dessus a pour plus général unificateur $\{x_1 \mapsto t_1; \ldots; x_n \mapsto t_n\}$.

Proposition 3.6.4 *Tout problème d'unification qui ne peut être simplifié par les règles de la figure 3.3 est en arbre-forme résolue.*

Exercice 96
Prouver la proposition 3.6.4. Indiquer un sous-ensemble des règles qui est nécessaire et suffisant pour obtenir ce résultat.

Théorème 3.6.1 (Robinson) *Il y a un algorithme qui, étant donné un problème d'unification P,*

- *soit répond « non », et dans ce cas P n'a pas d'unificateur ;*
- *soit donne une substitution σ, et dans ce cas σ est un mgu de P.*

Preuve:
Étant donné un problème d'unification P, on applique les règles de la Figure 3.3 dans un ordre quelconque. Par la Proposition 3.6.3, on obtient en temps fini un problème d'unification P' sur lequel aucune règle d'unification s'applique. Par la Proposition 3.6.2, P et P' ont les mêmes unificateurs. Par la Proposition 3.6.4 il y a deux possibilités :

1. P' est $\bot$. Par Proposition 3.6.2, P n'a pas d'unificateur.
2. P' est de la forme $x_1 \stackrel{?}{=} t_1 \wedge \ldots \wedge x_n \stackrel{?}{=} t_n$, et les variables $x_1, \ldots, x_n$ sont éliminées en P. Dans ce cas, $\sigma = \{x_1 \to t_1; \ldots, x_n \to t_n\}$ est un mgu de P', donc par Proposition 3.6.2 aussi de P.

$\square$

Exercice 97
Calculer un mgu pour les problèmes d'unification suivants :

1. $f(x, g(a, y)) \stackrel{?}{=} f(h(y), g(y, a)) \wedge g(x, h(y)) \stackrel{?}{=} g(z, z))$
2. $f(x, x) \stackrel{?}{=} f(g(y), z) \wedge h(z) \stackrel{?}{=} h(y)$

Definition 3.6.3 *Un problème d'unification est en DAG-forme résolue si c'est* $\top, \bot$ *ou bien* $x_1 \stackrel{?}{=} t_1 \wedge \ldots \wedge x_n \stackrel{?}{=} t_n$ *où* $x_1, \ldots, x_n$ *sont des variables distinctes telles que,* $\forall i, \forall j \geq i, x_i \notin Var(t_j)$.

Exercice 98

1. Montrer qu'une DAG forme résolue comme ci-dessus définit un mgu $\{x_1 \mapsto t_1\} \cdots \{x_n \mapsto t_n\}$.
2. Montrer que, pour tout n, il est possible que $|t_1| + ... + |t_n| = O(n)$ alors que tout mgu $\{y_1 \mapsto u_1; \ldots ; y_k \mapsto u_k\}$ est exponentiellement plus grand $(|u_1| + \ldots + |u_k| = O(2^n))$.

Exercice 99
Donner un sous-ensemble minimal de règles de la figure 3.3 tel que tout problème irréductible pour ces règles soit en DAG-forme résolue (justifier à la fois la minimalité et le fait que les règles soient suffisantes).

Definition 3.6.4 *Un* cycle de variables *est une conjonction d'équations* $x_1 \stackrel{?}{=} x_2 \wedge \ldots \wedge x_n \stackrel{?}{=} x_1$.

Un problème d'unification est en RT-forme résulue si c'est $\bot, \top$ *ou bien une conjonction* $x_1 \stackrel{?}{=} t_1 \wedge \ldots \wedge x_n \stackrel{?}{=} t_n$ *qui ne contient pas de cycle de variable et tel que* $x_1, \ldots, x_n$ *sont des variables distinctes.*

Exercice 100

1. Donner un sous-ensemble minimal de règles de la figure 3.3 qui garantisse que les problèmes irréductibles sont en RT-forme résolue.
2. Montrer que ces règles sont correctes si on interprète les problèmes d'unification dans l'algèbre des termes finis ou infinis.
3. Montrer que toute RT-forme résolue a une solution dans la F-algèbre des termes finis ou infinis.
4. Comment définir un mgu dans cette algèbre ? Pourquoi l'obtient on avec les règles de la figure 3.3 ?

Exercice 101 (6)
On appelle *anti-unificateur* de deux termes u et v, un terme t tel qu'il existe une substitution σ et il existe une substitution θ telles que $u = t\sigma$ et $v = t\theta$.

Montrer que toute paire de termes possède un moins général (ou plus spécialisé) anti-unificateur. Donner un algorithme qui permette de le calculer.

(Note : en fait, modulo similarité, le préordre d'instanciation muni l'algèbre des termes d'un structure de treillis. L'inf est calculé par anti-unification et le sup par unification).