Licence Informatique, semestre 5 — 2019–20
Eléments de logique pour l'informatique (Info 315) — 24 novembre 2019
`http://www.lri.fr/~paulin/Logique`

Feuille 7 - Skolémisation, Modèles de Herbrand, Unification

Exercice 1 Mettre sous forme clausale l'ensemble de formules $E = \{F_1, F_2, F_3\}$ où

1. $F_1 = \forall x, (p(x) \Rightarrow \exists y, \forall x, q(x, y))$
2. $F_2 = ((\exists x, (p(x) \Rightarrow r(x))) \vee \forall y,\ p(y)) \wedge \forall x, \exists y, (r(y) \Rightarrow p(x))$
3. $F_3 = ((\forall x, (p(x) \Rightarrow \exists y, q(y))) \Rightarrow \exists z, r(z)) \Rightarrow \exists u, s(u)$

Exercice 2 *Satisfiabilité, examen 2 2013*
Soit la formule $A \stackrel{\text{def}}{=} (\exists x, \neg P(x)) \Rightarrow ((\forall x, P(x) \vee Q(x)) \Rightarrow \forall x, Q(x))$

1. Mettre la formule A en forme normale de négation (les négations ne portent que sur les prédicats et il n'y a plus de connecteur d'implication).
2. Soit B la formule obtenue à la question précédente, dire si les affirmations suivantes sont vraies ou fausses (sans les justifier, c'est du cours !)
   — $A \models B$
   — $B \models A$
   — A est satisfiable si et seulement si B l'est.
3. Eliminer dans B les quantificateurs existentiels ($\exists$) en utilisant la skolémisation et mettre les quantificateurs universels ($\forall$) en tête de la formule.
4. Soit C la formule obtenue à la question précédente, dire si les affirmations suivantes sont vraies ou fausses (sans les justifier, c'est du cours !)
   — $B \models C$
   — $C \models B$
   — B est satisfiable si et seulement si C l'est.
5. La formule C est-elle vraie dans un modèle dont le domaine a exactement un élément ? Même question pour A, justifier vos réponses.
6. La formule A est-elle satisfiable ?
7. Mettre la formule $\neg A$ en forme clausale.
8. Indiquer le domaine et la base de Herbrand pour la forme clausale ainsi obtenue.
9. La formule $\neg A$ est-elle satisfiable ? La formule A est-elle valide ?

Exercice 3 Le domaine de Herbrand est formé des termes clos (sans variable) construits à partir de la signature. Chaque symbole de fonction est interprété par lui-même.

Pour les formules suivantes : donner le domaine de Herbrand et dire si les formules sont satisfiables.

1. $\forall x, (P(x) \wedge Q(x) \wedge (\neg P(a) \vee \neg Q(b)))$
2. $\forall x, ((P(x) \vee Q(x)) \wedge \neg P(a) \wedge \neg Q(b))$
3. $\forall x, (P(x) \wedge \neg P(f(x)))$
4. $\forall xyz, (R(x, s(x)) \wedge (R(x, y) \wedge R(y, z) \Rightarrow R(x, z)) \wedge \neg R(x, x))$

Exercice 4 Pour chaque ensemble de formules suivantes : donner la signature du langage, le domaine de Herbrand et dire si l'ensemble de formules est satisfiable ou non.

1. $\{\forall x, (P(x) \vee Q(x) \vee R(x)); \neg P(a); \neg Q(b); \neg R(c)\}$
2. $\{\forall x, P(x); \forall x, \neg Q(x); \forall x, (\neg P(f(x)) \vee Q(f(x)))\}$

3. $\{\forall x, P(x); \forall x, \neg P(f(x)); \forall x, P(f(f(x))); \forall x, (\neg P(f(f(x))) \vee \neg P(x) \vee P(f(x)))\}$

Exercice 5 *Forme de Herbrand*

On rappelle que le théorème de Skolem dit que pour toute formule close A, il existe une formule B de la forme $\forall x_1 \dots x_n, C$ avec C sans quantificateur telle que les trois propriétés suivantes soient vérifiées

1. $B \models A$,
2. si A est satisfiable alors B est satisfiable
3. si A est insatisfiable alors il existe des substitutions closes $\sigma_1, \dots, \sigma_k$ telles que $\{C[\sigma_1], \dots, C[\sigma_k]\}$ soit insatisfiable.

A partir de ce résultat, et de la correspondance entre validité d'une formule et insatisfiabilité de sa négation, montrer le résultat dual suivant

1. Pour une formule P close quelconque, montrer qu'il existe une formule Q (appelée forme de Herbrand de P) qui s'écrit $\exists x_1 \dots x_n, R$ avec R sans quantificateur telle que les trois propriétés suivantes sont vérifiées
   (a) $P \models Q$,
   (b) si Q est valide alors P est valide
   (c) si P est valide alors il existe des substitutions closes $\sigma_1, \dots, \sigma_k$ telles que la formule $R[\sigma_1] \vee \dots \vee R[\sigma_k]$ soit valide.
2. Montrer que $R[\sigma_1] \vee \dots \vee R[\sigma_k] \Rightarrow Q$ est une formule valide.
3. Soit la formule $P \stackrel{\text{def}}{=} (T(a) \vee T(b)) \Rightarrow \exists x, T(x)$, trouver la forme de Herbrand associée ainsi que des substitutions closes $\sigma_1, \dots, \sigma_k$ telles que $R[\sigma_1] \vee \dots \vee R[\sigma_k]$ soit valide. Peut-on trouver une solution à ce problème avec une seule substitution.

Exercice 6 *Exercice théorique optionnel.* Le but de l'exercice est de montrer que dans un langage contenant uniquement m constantes $c_1, \dots, c_m$ avec $(1 \leq m)$ et pas de fonction, alors une formule $\forall x_1 \dots x_n, \exists y_1 \dots y_p, A$ avec A sans quantificateur est valide si elle est vraie dans toute interprétation qui a moins de $n + m$ éléments.

1. Peut-on utiliser le théorème d'Herbrand pour justifier ce résultat ?
2. Soit deux interprétations I et J d'une même signature. On dit que J est une sous-interprétation de I si
   — le domaine E de J est inclus dans le domaine D de I
   — l'interprétation f_J d'un symbole f dans J est la restriction à E de l'interprétation f_I du symbole f dans I (en particulier l'interprétation des constantes est la même et appartient donc à E).
   — l'interprétation R_J d'un symbole de relation R dans J est la restriction à E de l'interprétation R_I du symbole R dans I, c'est-à-dire que $R_J = \{(u_1, \dots, u_n) \in E^n | R_I(u_1, \dots, u_n)\}$

   Soit J une sous-interprétation de I et e un environnement dans J. Montrer les résultats suivants :
   (a) $\texttt{val}_I(e, t) = \texttt{val}_J(e, t)$
   (b) Si A est une formule sans quantificateur alors
      i. $\texttt{val}_I(e, A) = \texttt{val}_J(e, A)$ pour tout terme t du langage
      ii. Si $\texttt{val}_I(e, \forall x_1 \dots x_n, A) = V$ alors $\texttt{val}_J(e, \forall x_1 \dots x_n, A) = V$
      iii. Si $\texttt{val}_J(e, \exists x_1 \dots x_n, A) = V$ alors $\texttt{val}_I(e, \exists x_1 \dots x_n, A) = V$
      iv. Donner un exemple qui montre que les réciproques des deux derniers réultats sont fausses.
3. On se donne un langage contenant uniquement m constantes $c_1, \dots, c_m$ avec $(1 \leq m)$ et pas de fonction et une formule $B \stackrel{\text{def}}{=} \forall x_1 \dots x_n, \exists y_1 \dots y_p, A$ avec A sans quantificateur et on suppose que cette formule est vraie dans toute interprétation de cardinal inférieur à $n + m$.

   Soit $I = (D, F_I, R_I)$ une interprétation et $m_1, \dots, m_n \in D$, soit J la sous interprétation de I construite en restreignant I sur le domaine $E \stackrel{\text{def}}{=} \{m_1, \dots, m_n\} \cup F_I$.
   (a) Donner une borne du cardinal du domaine de J et en déduire que B est vrai dans J.
   (b) En déduire que B est vraie dans I
4. Montrer que ce résultat n'est plus vrai si le langage contient un symbole de fonction.

Exercice 7 *Filtrage*

On rappelle qu'étant donné un *motif* p (terme n'ayant pas deux fois la même variable), on note $\texttt{inst}(p)$ l'ensemble des instances closes de p, c'est-à-dire les termes clos (sans variable) de la forme $p[\sigma]$.

On considère une signature pour représenter des nombres avec deux symboles binaires `plus` et `mult`, deux symboles unaires `opp` et `inv` et deux constantes `zero` et `un`. Soit la fonction

```
let rec simpl e = match e with
   plus(x,zero) | plus(zero,x) -> x
 | mult(zero,x) | mult(x,zero) -> zero
 | mult(un,x)   | mult(x,un)   -> x
```

1. Les motifs de la définition sont-ils disjoints ? complets ?
2. Sur cette signature, proposer un algorithme `inter` qui étant donnés deux motifs p et q construit un motif r tel que $\texttt{inst}(r) = \texttt{inst}(p) \cap \texttt{inst}(q)$ ou renvoie $\emptyset$ si l'intersection est vide.
3. De même proposer un algorithme `compl` qui étant donné un motif p construit un ensemble de motifs disjoints $\{p_1, \ldots, p_n\}$ qui correspond au complémentaire du motif p, c'est-à-dire tel que $\bigcup_{i=}^{n} \texttt{inst}(p_i) = \mathcal{T}(\mathcal{F}) \setminus \texttt{inst}(p)$.
4. Expliquer comment, en utilisant ces fonctions, on peut transformer la définition précédente pour n'avoir que des motifs disjoints, et détecter les définitions incomplètes.
5. Comment peut-on repérer qu'un des cas est inutile ?

Exercice 8 *Unification* Soit p un symbole de prédicat binaire, q un symbole de prédicat ternaire, r un symbole de prédicat quaternaire, f, g, h trois symboles de fonction unaire, k un symbole de fonction binaire, a et b deux constantes et v, w, x, y, z des symboles de variable. Calculer s'il existe, l'unificateur principal des paires d'atomes (A_1, A_2) suivantes en appliquant l'algorithme d'unification vu en cours.

$$\begin{array}{llll}
A_1 : & q(a, x, f(g(y))) & A_2 : & q(z, f(z), f(w)) \\
A_1 : & p(f(a), g(x)) & A_2 : & p(y, y) \\
A_1 : & p(x, k(y, z)) & A_2 : & p(x, f(g(h(x)))) \\
A_1 : & q(x, f(x), k(f(x), x)) & A_2 : & q(z, f(f(a)), k(f(k(a, z)), y)) \\
A_1 : & q(f(k(x, y)), k(v, w), y) & A_2 : & q(f(z), x, f(y)) \\
A_1 : & q(x, f(x), f(f(x))) & A_2 : & q(f(f(y)), y, f(y)) \\
A_1 : & r(f(y), f(z), f(w), f(x)) & A_2 : & r(g(z), g(x), g(y), g(z))
\end{array}$$

Exercice 9 *Complexité de l'algorithme de Robinson.*

On considère une suite de variables $(x_n)_{n \in \mathbb{N}}$ et une signature avec un symbole de fonction binaire f. Soit les deux suites de termes

$$u_0 = x_0 \qquad u_{n+1} = f(u_n, x_n) \qquad v_0 = x_0 \qquad v_{n+1} = f(x_n, v_n)$$

1. appliquer l'algorithme d'unification au problème $u_n \stackrel{?}{=} v_n$, on pourra d'abord regarder le problème $u_0 \stackrel{?}{=} v_0$ puis le problème $u_{n+1} \stackrel{?}{=} v_{n+1}$ en supposant que l'on sait résoudre $u_n \stackrel{?}{=} v_n$.
2. quelle est la taille du terme solution ?
3. compter le nombre d'étapes nécessaires à l'unification des termes $f(u_n, u_n) \stackrel{?}{=} f(v_n, v_n)$

Exercice 10 *Correction de l'unification.* Soit le problème d'unification $E \stackrel{\text{def}}{=} \{x \stackrel{?}{=} t; u \stackrel{?}{=} v\}$ tel que la variable x n'est pas libre dans les termes t, u et v. Soit σ l'unificateur principal de u et v. Soit $\tau \stackrel{\text{def}}{=} \sigma \circ \{x \leftarrow t\}$,

1. exprimer la valeur de $\tau(z)$ en fonction de t et σ lorsque $z = x$, et lorsque z est une variable différente de x
2. comparer $p[\tau]$ et $p[\sigma]$ lors que x n'est pas une variable libre du terme p
3. montrer que τ est l'unificateur principal de E.