Base de la démonstration automatique : Théorème de Herbrand

Stéphane Devismes Pascal Lafourcade Michel Lévy

Université Joseph Fourier, Grenoble I

25 novembre 2008

Plan

Plan

Introduction

Rappel : En logique du premier ordre, il n'a pas d'algorithme pour décider si une formule est valide ou non valide.

Introduction

Rappel : En logique du premier ordre, il n'a pas d'algorithme pour décider si une formule est valide ou non valide.

Mais on peut d'écrire un programme (*semi-décidable*), qui a pour donnée une formule et qui a le comportement suivant :

1. il termine en déclarant la formule valide (cette déclaration étant souvent accompagnée d'une preuve de la formule).
2. il termine en déclarant qu'il n'y a pas de preuve de la formule, donc qu'elle n'est pas valide.
3. il termine après épuisement des ressources allouées au programme sans donner de réponse : on ne sait pas alors le statut de la formule.

Introduction

Rappel : En logique du premier ordre, il n'a pas d'algorithme pour décider si une formule est valide ou non valide.

Mais on peut d'écrire un programme (*semi-décidable*), qui a pour donnée une formule et qui a le comportement suivant :

1. il termine en déclarant la formule valide (cette déclaration étant souvent accompagnée d'une preuve de la formule).
2. il termine en déclarant qu'il n'y a pas de preuve de la formule, donc qu'elle n'est pas valide.
3. il termine après épuisement des ressources allouées au programme sans donner de réponse : on ne sait pas alors le statut de la formule.

Nous étudions maintenant un tel programme basés sur la *résolution*.

Plan

Fermeture universelle

Soit C une formule ayant pour variables libres $x_1, \ldots x_n$.

La fermeture universelle de C, notée $\forall(C)$, est la formule $\forall x_1 \ldots \forall x_n C$. Cette notion est définie à l'ordre près des variables libres de C.

Soit Γ un ensemble de formules, $\forall(\Gamma) = \{\forall(A) \mid A \in \Gamma\}$

Fermeture universelle

Soit C une formule ayant pour variables libres $x_1, \ldots x_n$.

La fermeture universelle de C, notée $\forall(C)$, est la formule $\forall x_1 \ldots \forall x_n C$.
Cette notion est définie à l'ordre près des variables libres de C.

Soit Γ un ensemble de formules, $\forall(\Gamma) = \{\forall(A) \mid A \in \Gamma\}$

$$\forall(P(x) \wedge R(x,y)) = \forall x \forall y (P(x) \wedge R(x,y)) = \forall y \forall x (P(x) \wedge R(x,y))$$

Plan

Hypothèses

A partir de maintenant, on ne considére que des formules qui ne contiennent pas le symbole égal, dont le sens est fixé dans toute interprétation.

De plus on considère que toute signature comporte au moins une constante.

Ainsi la signature d'un ensemble de formules ne comportant pas de constante, sera complétée par **la constante *a***.

Domaine et base de Herbrand

Domaine et base de Herbrand

1. Le domaine de Herbrand pour Σ est l'ensemble des termes fermés (*i.e.*, sans variable) de cette signature.

   On le note D_Σ.

Domaine et base de Herbrand

1. Le domaine de Herbrand pour Σ est l'ensemble des termes fermés (*i.e.*, sans variable) de cette signature.

   On le note $\boldsymbol{D_\Sigma}$.

   Remarque : Puisque la signature comporte au moins une constante, cet ensemble n'est jamais vide.

Domaine et base de Herbrand

1. Le domaine de Herbrand pour Σ est l'ensemble des termes fermés (*i.e.*, sans variable) de cette signature.

   On le note $\boldsymbol{D_\Sigma}$.

   Remarque : Puisque la signature comporte au moins une constante, cet ensemble n'est jamais vide.

2. La base de Herbrand pour Σ est l'ensemble des formules atomiques fermées (sauf $\top$ et $\bot$) de cette signature.

   On la note $\boldsymbol{B_\Sigma}$.

Exemple

Exemple

1. Soit Σ la signature comportant uniquement les 2 constantes a, b et les 2 symboles de relations unaires P, Q.

   On a $D_\Sigma = \{a, b\}$ et $B_\Sigma = \{P(a), P(b), Q(a), Q(b)\}$.

Exemple

1. Soit Σ la signature comportant uniquement les 2 constantes a, b et les 2 symboles de relations unaires P, Q.

   On a $D_\Sigma = \{a, b\}$ et $B_\Sigma = \{P(a), P(b), Q(a), Q(b)\}$.

2. Soit Σ la signature comportant uniquement la constante a, le symbole de fonction unaire f et le symbole de relation unaire P.

   On a $D_\Sigma = \{f^n(a) \mid n \in \mathbb{N}\}$ et $B_\Sigma = \{P(f^n(a)) \mid n \in \mathbb{N}\}$

Interprétation de Herbrand

Soit Σ une signature et $E \subseteq B_\Sigma$.

L'interprétation de Herbrand $H_{\Sigma,E}$ a pour domaine D_Σ et donne aux symboles le sens suivant :

1. Si le symbole s est une constante de la signature , il vaut lui-même dans cette interprétation.
2. si $n \geq 1$ et si s est un symbole de fonction à n arguments de la signature et si $t_1, \ldots t_n \in D_\Sigma$ alors $s^{fn}_{H_{\Sigma,E}}(t_1, \ldots t_n) = s(t_1, \ldots t_n)$
3. Si le symbole s est une variable propositionnelle, il vaut 1, autrement dit il est vrai, si et seulement si $s \in E$
4. si $n \geq 1$ et si s est un symbole de relation de la signature et si $t_1, \ldots t_n \in D_\Sigma$ alors $s^{rn}_{H_{\Sigma,E}} = \{(t_1, \ldots t_n) \mid t_1, \ldots t_n \in D_\Sigma \wedge s(t_1, \ldots t_n) \in E\}$

Propriété de l'interprétation de Herbrand

Soit Σ une signature et $E \subseteq B_\Sigma$. Dans l'interprétation de Herbrand $H_{\Sigma,E}$,

1. La valeur d'un terme sans variable est lui-même
2. L'interprétation est modèle d'une formule atomique fermée (sauf $\top$ et $\bot$) si et seulement si cette formule est élément de E

Exemple

Soit Σ la signature comportant les 2 constantes a, b et les 2 symboles de relations unaires P, Q.

L'ensemble $E = \{P(b), Q(a)\}$ définit l'interprétation de Herbrand H de domaine $D_\Sigma = \{a, b\}$ où :

- les constantes a et b ont pour valeur elles-mêmes et
- $P_H = \{b\}$ et $Q_H = \{a\}$.

Formule universelle et modèle de Herbrand

Soit Γ un ensemble de formules sans quantificateurs sur la signature Σ.

$\forall(\Gamma)$ a un modèle si et seulement si $\forall(\Gamma)$ a un modèle qui est une interprétation de Herbrand de Σ.

Plan

Théorème de Herbrand

Soit Γ un ensemble de formules sans quantificateur de signature Σ.

$\forall(\Gamma)$ a un modèle *si et seulement si* tout ensemble fini d'instances fermées sur la signature Σ des formules de Γ a un modèle propositionnel application de la base de Herbrand B_Σ dans l'ensemble $\{0, 1\}$.

Rappel : On rappelle que l'on suppose que la signature comporte au moins une constante et que le signe égal n'est pas utilisé.

Idées de la preuve

$\Rightarrow$ Supposons que $\forall(\Gamma)$ a un modèle I. Les instances des formules de Γ sont conséquences de $\forall(\Gamma)$ donc ont pour modèle I. Ce modèle I peut être vu comme une modèle propositionnel v de domaine B_Σ, la base de Herbrand de la signature Σ, où pour tout $A \in B_\Sigma$, $v(A) = [A]_I$.
Donc v est modèle propositionnel de tout ensemble d'instances des formules de Γ.

Idées de la preuve

- $\Rightarrow$ Supposons que $\forall(\Gamma)$ a un modèle I. Les instances des formules de Γ sont conséquences de $\forall(\Gamma)$ donc ont pour modèle I. Ce modèle I peut être vu comme une modèle propositionnel v de domaine B_Σ, la base de Herbrand de la signature Σ, où pour tout $A \in B_\Sigma$, $v(A) = [A]_I$.
  Donc v est modèle propositionnel de tout ensemble d'instances des formules de Γ.
- $\Leftarrow$ Supposons que tout ensemble *fini* d'instances fermées sur la signature Σ des formules de Γ a un modèle propositionnel de domaine B_Σ. On démontre que de l'ensemble de *toutes* les instances fermées sur la signature Σ a alors un modèle propositionnel v de domaine B_Σ.
  Ce modèle propositionnel peut être vu comme le modèle de Herbrand de $\forall(\Gamma)$ associé à l'ensemble des élements de la base de Herbrand dont v est modèle.

Variante du théorème de Herbrand

Soit Γ un ensemble de formules sans quantificateur de signature Σ.

$\forall(\Gamma)$ est insatisfaisable *si et seulement si* il existe un ensemble fini insatisfaisable d'instances fermées sur la signature Σ des formules de Γ.

Variante du théorème de Herbrand

Soit Γ un ensemble de formules sans quantificateur de signature Σ.

$\forall(\Gamma)$ est insatisfaisable *si et seulement si* il existe un ensemble fini insatisfaisable d'instances fermées sur la signature Σ des formules de Γ.

Remarque : cette variante est obtenue en remplaçant chaque côté de l'équivalence du théorème de Herbrand par sa négation.

Algorithme

Dans le cas où Γ est un ensemble *fini* de formules, le corollaire précédent fonde une procédure de *semi-décision* pour savoir si $\forall(\Gamma)$ est ou n'est pas insatisfaisable :

On enumère l'ensemble des instances fermées des formules de Γ sur la signature Σ et on arrête cette énumération dès qu'on obtient un ensemble insatisfaisable, ou dès que cette enumération est terminée sans contradiction ou dès qu'on est « fatigué » !

Algorithme

Dans le cas où Γ est un ensemble *fini* de formules, le corollaire précédent fonde une procédure de *semi-décision* pour savoir si $\forall(\Gamma)$ est ou n'est pas insatisfaisable :

On enumère l'ensemble des instances fermées des formules de Γ sur la signature Σ et on arrête cette énumération dès qu'on obtient un ensemble insatisfaisable, ou dès que cette enumération est terminée sans contradiction ou dès qu'on est « fatigué » !

1. Dans le premier cas, la procédure répond que $\forall(\Gamma)$ est insatisfaisable.

Algorithme

Dans le cas où Γ est un ensemble *fini* de formules, le corollaire précédent fonde une procédure de *semi-décision* pour savoir si $\forall(\Gamma)$ est ou n'est pas insatisfaisable :

On enumère l'ensemble des instances fermées des formules de Γ sur la signature Σ et on arrête cette énumération dès qu'on obtient un ensemble insatisfaisable, ou dès que cette enumération est terminée sans contradiction ou dès qu'on est « fatigué » !

1. Dans le premier cas, la procédure répond que $\forall(\Gamma)$ est insatisfaisable.
2. Le deuxième cas ne peut se produire que si le domaine de Herbrand ne comprend que des constantes, la procédure répond que $\forall(\Gamma)$ est satisfaisable et en donne un modèle.

Algorithme

Dans le cas où Γ est un ensemble *fini* de formules, le corollaire précédent fonde une procédure de *semi-décision* pour savoir si $\forall(\Gamma)$ est ou n'est pas insatisfaisable :

On enumère l'ensemble des instances fermées des formules de Γ sur la signature Σ et on arrête cette énumération dès qu'on obtient un ensemble insatisfaisable, ou dès que cette enumération est terminée sans contradiction ou dès qu'on est « fatigué » !

1. Dans le premier cas, la procédure répond que $\forall(\Gamma)$ est insatisfaisable.
2. Le deuxième cas ne peut se produire que si le domaine de Herbrand ne comprend que des constantes, la procédure répond que $\forall(\Gamma)$ est satisfaisable et en donne un modèle.
3. Dans le troisième cas, on ne peut pas conclure : le corollaire nous dit que si $\forall(\Gamma)$ est insatisfaisable, et si l'on avait été plus courageux, on aurait obtenu une contradiction !

Exemple (1/5)

Soit $\Gamma = \{P(x), Q(x), \neg P(a) \vee \neg Q(b)\}$.

La signature Σ comporte 2 constantes a, b et 2 symboles de relation unaire P, Q.

Exemple (1/5)

Soit $\Gamma = \{P(x), Q(x), \neg P(a) \vee \neg Q(b)\}$.

La signature Σ comporte 2 constantes a, b et 2 symboles de relation unaire P, Q.

Le domaine de Herbrand est $\{a, b\}$.

Exemple (1/5)

Soit $\Gamma = \{P(x), Q(x), \neg P(a) \vee \neg Q(b)\}$.

La signature Σ comporte 2 constantes a, b et 2 symboles de relation unaire P, Q.

Le domaine de Herbrand est $\{a, b\}$.

L'ensemble $\{P(a), Q(b), \neg P(a) \vee \neg Q(b)\}$ d'instances sur le domaine de Herbrand est insatisfaisable, donc $\forall(\Gamma)$ est insatisfaisable.

Exemple (2/5)

Soit $\Gamma = \{P(x) \vee Q(x), \neg P(a), \neg Q(b)\}$.

Exemple (2/5)

Soit $\Gamma = \{P(x) \vee Q(x), \neg P(a), \neg Q(b)\}$.

On a la même signature que précédemment.

Exemple (2/5)

Soit $\Gamma = \{P(x) \vee Q(x), \neg P(a), \neg Q(b)\}$.

On a la même signature que précédemment.

L'ensemble de *toutes* les instances sur le domaine de Herbrand $\{P(a) \vee Q(a), P(b) \vee Q(b), \neg P(a), \neg Q(b)\}$ a un modèle propositionnel caractérisé par $E = \{P(b), Q(a)\}$.

Donc l'interprétation de Herbrand associée à E est modèle de $\forall(\Gamma)$.

Exemple (3/5)

Soit $\Gamma = \{P(x), \neg P(f(x))\}$.

Exemple (3/5)

Soit $\Gamma = \{P(x), \neg P(f(x))\}$.

La signature Σ comporte une constante a , un symbole de fonction unaire f et un symbole de relation unaire P.

Remarque : la constante a est ajoutée à la signature de Γ pour que le domaine de Herbrand ne soit pas vide.

Exemple (3/5)

Soit $\Gamma = \{P(x), \neg P(f(x))\}$.

La signature Σ comporte une constante a , un symbole de fonction unaire f et un symbole de relation unaire P.

Remarque : la constante a est ajoutée à la signature de Γ pour que le domaine de Herbrand ne soit pas vide.

L'ensemble $\{P(f(a)), \neg P(f(a))\}$ d'instances sur le domaine de Herbrand est insatisfaisable, donc $\forall(\Gamma)$ est insatisfaisable.

Exemple (4/5)

Soit $\Gamma = \{P(x) \vee \neg P(f(x)), \neg P(a), P(f(f(a)))\}$.

Exemple (4/5)

Soit $\Gamma = \{P(x) \vee \neg P(f(x)), \neg P(a), P(f(f(a)))\}$.

On a la même signature que précédemment.

Exemple (4/5)

Soit $\Gamma = \{P(x) \vee \neg P(f(x)), \neg P(a), P(f(f(a)))\}$.

On a la même signature que précédemment.

L'ensemble
$\{P(a) \vee \neg P(f(a)), P(f(a)) \vee \neg P(f(f(a))), \neg P(a), P(f(f(a)))\}$
d'instances sur le domaine de Herbrand est insatisfaisable, donc $\forall(\Gamma)$ est insatisfaisable.

Exemple (4/5)

Soit $\Gamma = \{P(x) \vee \neg P(f(x)), \neg P(a), P(f(f(a)))\}$.

On a la même signature que précédemment.

L'ensemble
$\{P(a) \vee \neg P(f(a)), P(f(a)) \vee \neg P(f(f(a))), \neg P(a), P(f(f(a)))\}$
d'instances sur le domaine de Herbrand est insatisfaisable, donc $\forall(\Gamma)$ est insatisfaisable.

Remarque : observez qu'il a fallu prendre 2 instances de la première formule de Γ pour obtenir une contradiction.

Exemple (5/5)

Soit $\Gamma = \{R(x, s(x)), R(x, y) \wedge R(y, z) \Rightarrow R(x, z), \neg R(x, x)\}$.

Exemple (5/5)

Soit $\Gamma = \{R(x, s(x)), R(x, y) \wedge R(y, z) \Rightarrow R(x, z), \neg R(x, x)\}$.

La signature Σ comporte une constante a, un symbole de fonction unaire s et un symbole de relation binaire R.

Exemple (5/5)

Soit $\Gamma = \{R(x,s(x)), R(x,y) \wedge R(y,z) \Rightarrow R(x,z), \neg R(x,x)\}$.

La signature Σ comporte une constante a, un symbole de fonction unaire s et un symbole de relation binaire R.

Le domaine de Herbrand est $D_\Sigma = \{s^n(a) \mid n \in \mathbb{N}\}$. Ce domaine est infini.

Exemple (5/5)

Soit $\Gamma = \{R(x,s(x)), R(x,y) \wedge R(y,z) \Rightarrow R(x,z), \neg R(x,x)\}$.

La signature Σ comporte une constante a, un symbole de fonction unaire s et un symbole de relation binaire R.

Le domaine de Herbrand est $D_\Sigma = \{s^n(a) \mid n \in \mathbb{N}\}$. Ce domaine est infini.

$\forall(\Gamma)$ a un modèle infini : l'interprétation I de domaine $\mathbb{N}$ avec pour tout $n \in \mathbb{N}$,
$s_I(n) = n+1$ et
$R_I = \{(n,p) \mid n < p\}$, en bref $R(x,y) = x < y$.

Exemple (5/5)

Soit $\Gamma = \{R(x,s(x)), R(x,y) \wedge R(y,z) \Rightarrow R(x,z), \neg R(x,x)\}$.

La signature Σ comporte une constante a, un symbole de fonction unaire s et un symbole de relation binaire R.

Le domaine de Herbrand est $D_\Sigma = \{s^n(a) \mid n \in \mathbb{N}\}$. Ce domaine est infini.

$\forall(\Gamma)$ a un modèle infini : l'interprétation I de domaine $\mathbb{N}$ avec pour tout $n \in \mathbb{N}$,
$s_I(n) = n+1$ et
$R_I = \{(n,p) \mid n < p\}$, en bref $R(x,y) = x < y$.

$\forall(\Gamma)$ n'a aucun modèle fini, autrement dit il est inutile de chercher des modèles finis avec les méthodes du chapitre précédent.

Exemple (5/5)

Soit $\Gamma = \{R(x,s(x)), R(x,y) \wedge R(y,z) \Rightarrow R(x,z), \neg R(x,x)\}$.

La signature Σ comporte une constante a, un symbole de fonction unaire s et un symbole de relation binaire R.

Le domaine de Herbrand est $D_\Sigma = \{s^n(a) \mid n \in \mathbb{N}\}$. Ce domaine est infini.

$\forall(\Gamma)$ a un modèle infini : l'interprétation I de domaine $\mathbb{N}$ avec pour tout $n \in \mathbb{N}$,
$s_I(n) = n+1$ et
$R_I = \{(n,p) \mid n < p\}$, en bref $R(x,y) = x < y$.

$\forall(\Gamma)$ n'a aucun modèle fini, autrement dit il est inutile de chercher des modèles finis avec les méthodes du chapitre précédent.

Puisque $\forall(\Gamma)$ a un modèle, on est dans une situation, où la procédure évoquée ci-dessus, ne pourra jamais donner de réponses, aussi longtemps que l'on poursuive l'énumération des instances des formules de Γ.