

## TD 11 : Théorème de Herbrand

lionel.rieg@ens-lyon.fr

### Exercice 1 *Axiome atomique*

Dans le système LK réversible vu la semaine dernière, les axiomes  $\overline{\Gamma, A \vdash A, \Delta}$  portent sur des formules  $A$  arbitraires. Montrer qu'on peut se retréindre au cas où  $A$  doit être une formule atomique.

### Exercice 2 *Forme normale d'une preuve*

Dans la recherche automatique de preuves, on a intérêt à réduire au maximum l'espace de recherche donc à rechercher des preuves avec le plus de structure possible. Ainsi, l'élimination (ou la remontée) des coupures et la réversibilité participent à cet effort. Dans cet exercice, on va voir qu'on peut combiner ces résultats pour obtenir une forme très contrainte sur les preuves tout en restant complet. Le système de preuves que l'on va considérer est le système réversible vu la semaine dernière. On ne s'intéresse qu'aux formules en forme prénexé et on recherche des preuves sous la forme suivante :

- une partie réversible sans affaiblissement portant sur des formules sans quantificateur et avec axiome atomique,
- puis une partie avec des affaiblissements sur des formules quantifiées,
- enfin, une partie avec des introductions de quantificateurs et des contractions.

Noter qu'on travaille toujours à échange près.

1. Quel est l'intérêt de ne considérer que des formules en forme prénexé ?
2. On considère une preuve d'un séquent ne contenant que des formules en forme prénexé. Montrer que l'on peut faire remonter les affaiblissements au dessus des règles d'introduction des quantificateurs.
3. Pourquoi peut-on éviter les affaiblissements dans la partie réversible ?

## Théorème de Herbrand

L'énoncé auquel on va s'intéresser ici n'est pas celui que vous avez vu en cours :

Une formule  $\exists \vec{x}. F(\vec{x})$  (avec  $F$  sans quantificateur) est vraie  
si et seulement si elle possède une disjonction de Herbrand.

On va plutôt s'intéresser à l'équivalence entre des variantes des deux formules. Plus précisément, on part de la négation de  $\exists \vec{x}. F(\vec{x})$  : une formule universelle  $U$  (c'est à dire de la forme  $U = \forall \vec{x}. F'(\vec{x})$  où  $F' = \neg F$  est sans quantificateur). On va supposer qu'elle n'est pas satisfiable :

pour toute interprétation  $I$ ,  $I$  ne valide pas  $U$  i.e.  $\forall I. I \not\models U$

Pour le membre droit, on considère « la négation d'une disjonction de Herbrand », c'est-à-dire une conjonction d'instances closes de  $F' = \neg F$  qu'on suppose non valide (c'est-à-dire valide dans aucune interprétation). On montrera alors qu'elle est équivalente à  $\forall I. I \not\models U$ .

$\exists \vec{x}. F(\vec{x})$  est valide  $\stackrel{1}{\iff}$  pour toute interprétation  $I$ ,  $I \not\models U$   
 $\stackrel{2}{\iff}$  il existe  $t_1, \dots, t_n$  tels que  $F'(t_1) \wedge \dots \wedge F'(t_n)$  n'est valide dans aucune interprétation  
 $\stackrel{3}{\iff}$  il existe  $t_1, \dots, t_n$  tels que  $F(t_1) \vee \dots \vee F(t_n)$  est valide

**Exercice 3**      *Sens faciles*

1. Montrer l'équivalence 1.
2. Montrer l'équivalence 3.
3. Montrer le sens réciproque de l'équivalence 2.

Ne reste à montrer que le sens direct de l'équivalence 2, à savoir

Si pour toute interprétation  $\mathcal{I}$ ,  $\mathcal{I} \not\models U$ , alors il existe  $t_1, \dots, t_n$  tels que  $\not\models F'(t_1) \wedge \dots \wedge F'(t_n)$ .

La difficulté est de s'assurer que la conjonction contient suffisamment d'information pour couvrir toutes les interprétations  $\mathcal{I}$  possibles. Ces interprétations sont caractérisées par leurs valeurs sur les formules atomiques (le reste étant défini par les tables de vérité des connecteurs). Ainsi, pour s'assurer de couvrir toutes les interprétations, il suffit de couvrir toutes les fonctions de l'ensemble des instances closes des formules atomiques (la *base de Herbrand*  $\mathcal{B}$ ) dans les booléens.

Ainsi, chaque instance close  $f_i$  de  $F'$  dans la conjonction correspondra à une famille d'interprétations qui ont en commun la partie finie qui permet d'invalider  $f_i$ . Couvrir toutes les interprétations revient alors à s'assurer que toute interprétation possède une partie finie qui convient à l'un des  $f_i$ . On va voir que cela revient à montrer l'existence d'un *arbre de Herbrand*.

**Définition**      *Arbre de Herbrand*

Un *arbre de Herbrand* est un arbre binaire dont :

- les nœuds internes sont étiquetés par des atomes,
- les branches correspondent à des interprétations partielles finies,
- les feuilles contiennent des contradictions (des  $f_i$ ).

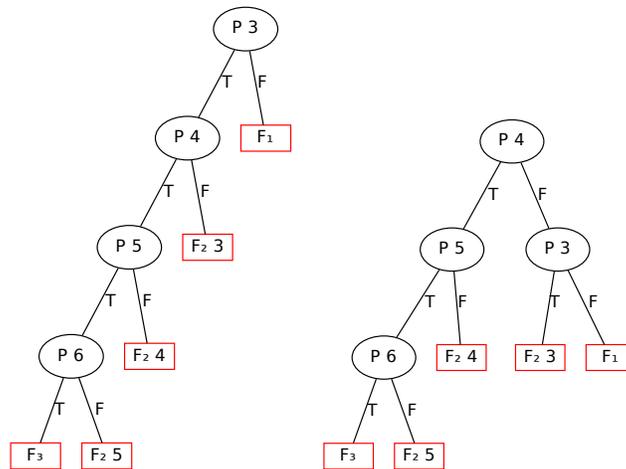
Par exemple, pour  $F = \neg P3 \vee (P x \wedge \neg P(x + 1)) \vee P6$ , une disjonction de Herbrand est

$$\neg P3 \vee (P3 \wedge \neg P4) \vee (P4 \wedge \neg P5) \vee (P5 \wedge \neg P6) \vee P6 .$$

On a alors  $F' = F_1 \wedge F_2 x \wedge F_3$  où

- $F_1 = P3$
- $F_2 x = P x \rightarrow P(x + 1)$
- $F_3 = \neg P6$

et voici ci-contre deux arbres de Herbrand :

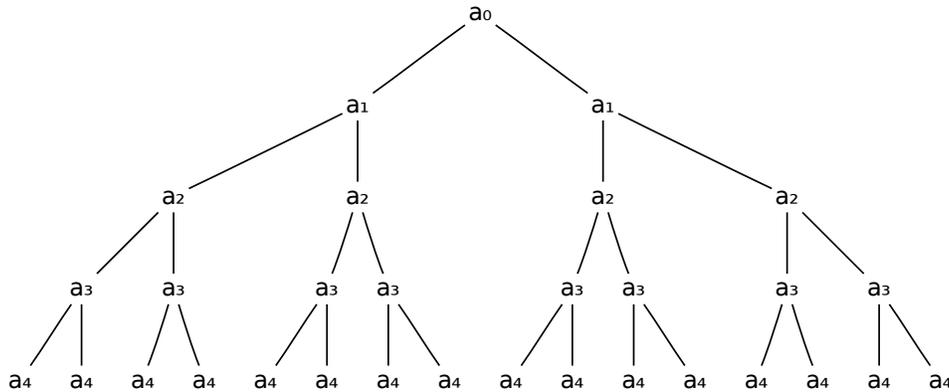


**Exercice 4** *Démonstration du théorème de Herbrand*

On veut démontrer la version du théorème de Herbrand présentée ci-avant.

1. Pourquoi la base de Herbrand  $\mathcal{B}$  est-elle dénombrable ?

On énumère alors les éléments de  $\mathcal{B}$  (appelés *atomes*) par  $(a_i)_{i \in \mathbb{N}}$  et on les représente dans un arbre binaire infini :



2. À quoi correspond une branche infinie dans cet arbre ?
3. En utilisant le théorème de compacité, montrer que l'on peut couper une branche infinie de cet arbre à profondeur finie et avoir une contradiction sur la feuille.
4. Utiliser le lemme de König faible pour conclure.

**Exercice 5** *Une preuve sans le lemme de König*

La preuve précédente comporte deux défauts. Son défaut capital est de nécessiter un ordre *a priori* sur les atomes qui peut être très mal adapté à la formule  $U$ . Le second est d'utiliser le lemme de König qui masque le contenu calculatoire de la preuve. On va donc dans cet exercice faire une autre preuve, par contraposition, qui évite ces deux écueils.

1. Comment vérifier calculatoirement qu'un arbre est bien un arbre de Herbrand (pour une formule  $U$  fixée) ?
2. Écrire l'énoncé (la contraposée du théorème) que l'on veut démontrer.
3. Montrer que si  $p$  ne possède pas de sous-arbre de Herbrand, alors  $p \cup \{a \mapsto true\}$  ou  $p \cup \{a \mapsto false\}$  ne possèdent pas de sous arbre de Herbrand.
4. En itérant ce procédé, construire une interprétation.
5. Montrer que cette interprétation est un modèle de  $U$ .

**Devoir Maison Coq pour le 20 décembre 2012**

Vous devez formaliser en Coq la seconde preuve du théorème de Herbrand vue dans ce TD. Vous avez droit à la logique classique (module `Classical`) mais aucun autre axiome. Ainsi, un `Print Assumptions Herbrand` à la fin du fichier ne doit renvoyer que `classic : forall P : Prop, P  $\vee$   $\sim$ P`.

Voici les types qui vont apparaître dans la formalisation :

|                              |  |
|------------------------------|--|
| <code>atom</code>            | les atomes (les instances close des formules atomiques)                          |
| <code>formula</code>         | les formules sans quantificateur   |
| <code>term</code>            | les termes du premier ordre (que l'on passe à $U = \forall \vec{x}. F \vec{x}$ ) |
| <code>path</code>            | les chemins dans un arbre binaire (= les interprétations finies)                 |
| <code>tree</code>            | les arbres de Herbrand   |
| <code>atom -&gt; Prop</code> | les interprétations  |

Pour simplifier, on va supposer `atom = nat` et `term = nat`. On veillera par contre dans la formalisation à utiliser `atom` et `term` plutôt que `nat` pour maintenir la distinction. Par ailleurs, la théorie  $U = \forall \vec{x}. F'(\vec{x})$  sera représentée par une fonction de `term` dans `formula`, c'est-à-dire on suppose qu'elle ne prend qu'un argument.

Vous trouverez un modèle sur la page des TD qui donne une méthode possible de démonstration. Vous êtes libre de ne pas le suivre mais le théorème que vous prouvez finalement doit être le même.

Quelques conseils pour finir :

- sur la page des TD, à côté du modèle `Herbrand.v` se trouve un fichier `OptBool.vo` qui définit des opérations sur le type `option bool` et prouve certains résultats qui peuvent vous être utiles ;
- on peut combiner plusieurs `destruct` en un seul en donnant un motif d'introduction :  
par exemple sur  $H : A \wedge (B \vee C)$ , on peut faire `destruct H as [HA [HB | HC]]` ;
- les réécritures (tactiques `rewrite` et `setoid_rewrite`) valent mieux que des `destruct` car elles ne polluent pas le contexte (au besoin, on peut faire `Require Import Setoid` auparavant) ;
- une induction sur un prédicat inductif permet d'avoir directement la bonne forme pour ses arguments et les hypothèses d'induction ;
- ne pas hésiter à m'envoyer un mail si vous avez des questions sur ce DM.

## Solutions

► **Exercice 1** La preuve se fait par induction sur  $A$  (en laissant  $\Gamma$  et  $\Delta$  variables).

- $A$  atomique : Il n’y a rien à faire.
- $A = B \wedge C$  : En utilisant les règles d’introduction de la conjonction et les hypothèses d’induction sur  $B$  et  $C$ , on obtient l’arbre de dérivation suivant :

$$\frac{\frac{\text{IH sur } B}{\Gamma, B, C \vdash B, \Delta} \quad \frac{\text{IH sur } C}{\Gamma, B, C \vdash C, \Delta}}{\Gamma, B, C \vdash B \wedge C, \Delta} \wedge_d \quad \frac{\Gamma, B, C \vdash B \wedge C, \Delta}{\Gamma, B \wedge C \vdash B \wedge C, \Delta} \wedge_g$$

- $A = B \vee C$  : Par dualité, on peut directement construire

$$\frac{\frac{\text{IH sur } B}{\Gamma, B \vdash B, C, \Delta} \quad \frac{\text{IH sur } C}{\Gamma, C \vdash B, C, \Delta}}{\Gamma, B \vee C \vdash B, C, \Delta} \vee_g \quad \frac{\Gamma, B \vee C \vdash B, C, \Delta}{\Gamma, B \vee C \vdash B \vee C, \Delta} \vee_d$$

- $A = B \rightarrow C$  : On procède de la même manière :

$$\frac{\frac{\text{IH sur } C}{\Gamma, C, B \vdash C, \Delta} \quad \frac{\text{IH sur } B}{\Gamma, B \vdash B, C, \Delta}}{\Gamma, B \rightarrow C, B \vdash C, \Delta} \rightarrow_g \quad \frac{\Gamma, B \rightarrow C, B \vdash C, \Delta}{\Gamma, B \rightarrow C \vdash B \rightarrow C, \Delta} \rightarrow_d$$

- $A = \neg B$  : Le dernier cas suit le même schéma :

$$\frac{\frac{\text{IH sur } B}{\Gamma, B \vdash B, \Delta}}{\Gamma, \neg B, B \vdash \Delta} \neg_g \quad \frac{\Gamma, \neg B, B \vdash \Delta}{\Gamma, \neg B \vdash \neg B, \Delta} \neg_d$$

► **Exercice 2**

1. Prendre des formules en forme préfixe permet de considérer des preuves sans règle de quantificateur au dessus d’une règle de connecteur. Ainsi, il n’y a pas besoin de montrer leur commutation (qui est fautive en logique intuitionniste).
2. Comme d’habitude, on travaille à échange près. Prenons par exemple une preuve sous la forme

$$\frac{\frac{\frac{\vdots}{\Gamma \vdash A, \Delta} \vee_d \quad x \notin FV(\Gamma, \Delta)}{\Gamma \vdash \forall x. A, \Delta} C}{\Gamma' \vdash \forall x. A, \Delta'} W_d \quad \frac{\Gamma' \vdash \forall x. A, \Delta'}{\Gamma' \vdash \forall x. A, B, \Delta'} W_d$$

⋮

Il faut faire attention au fait que  $A$  et  $B$  peuvent interagir dans la suite de la preuve par une contraction.

Quitte à  $\alpha$ -convertir, on suppose que les variables libres de  $B$  et  $A$  sont disjointes. On transforme cette preuve en

$$\frac{\frac{\frac{\frac{\vdots}{\Gamma \vdash A, \Delta} W_d}{\Gamma \vdash A, B, \Delta} W_d}{\Gamma \vdash \forall x. A, B, \Delta} \vee_d \quad x \notin FV(\Gamma, \Delta, B)}{\Gamma' \vdash \forall x. A, B, \Delta'} C \quad \frac{\Gamma' \vdash \forall x. A, B, \Delta'}{\Gamma' \vdash \forall x. A, B, \Delta'} C$$

⋮

Pour être plus précis, on commence par montrer que l'on peut faire remonter l'affaiblissement au dessus des contractions puis on montrera qu'on peut échanger la règle de quantificateur et la règle d'affaiblissement juste en dessous. On ne traite que le cas de deux règles droites mais les autres sont semblables.

$$\frac{\frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta} C_d}{\Gamma \vdash A, B, \Delta} W_d \quad \rightsquigarrow \quad \frac{\frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, A, B, \Delta} W_d}{\Gamma \vdash A, B, \Delta} C_d$$

Une fois que l'affaiblissement est remonté jusqu'à la règle de quantificateur, il ne reste qu'à échanger les deux. On suppose que  $x \notin FV(B)$ , quitte à  $\alpha$ -convertir  $A$ .

$$\frac{\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash \forall x. A, \Delta} \forall_d \quad x \notin FV(\Gamma, \Delta)}{\Gamma \vdash \forall x. A, B, \Delta} W_d \quad \rightsquigarrow \quad \frac{\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A, B, \Delta} W_d}{\Gamma \vdash \forall x. A, B, \Delta} \forall_d \quad x \notin FV(\Gamma, \Delta, B)$$

Les autres cas se traitent de façon similaires :

$$\begin{array}{ccc} \vdots & & \vdots \\ \frac{\frac{\Gamma, A[t/x] \vdash \Delta}{\Gamma, \forall x. A \vdash \Delta} \forall_g}{\frac{\Gamma', \forall x. A \vdash \Delta'}{\Gamma', \forall x. A, B \vdash \Delta'} W_g} C & \rightsquigarrow & \frac{\frac{\Gamma, A[t/x] \vdash \Delta}{\Gamma, A[t/x], B \vdash \Delta} W_g}{\frac{\Gamma, \forall x. A, B \vdash \Delta}{\Gamma', \forall x. A, B \vdash \Delta'} C} \forall_g \\ \vdots & & \vdots \\ \frac{\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash \exists x. A, \Delta} \exists_d}{\frac{\Gamma' \vdash \exists x. A, \Delta'}{\Gamma' \vdash \exists x. A, B, \Delta'} W_d} C & \rightsquigarrow & \frac{\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A, B, \Delta} W_d}{\frac{\Gamma \vdash \exists x. A, B, \Delta}{\Gamma' \vdash \exists x. A, B, \Delta'} C} \exists_d \\ \vdots & & \vdots \\ \frac{\frac{\Gamma, A \vdash \Delta}{\Gamma, \exists x. A \vdash \Delta} \exists_g \quad x \notin FV(\Gamma, \Delta)}{\frac{\Gamma', \exists x. A \vdash \Delta'}{\Gamma', \exists x. A, B \vdash \Delta'} W_g} C & \rightsquigarrow & \frac{\frac{\Gamma, A \vdash \Delta}{\Gamma, A, B \vdash \Delta} W_g}{\frac{\Gamma, \exists x. A, B \vdash \Delta}{\Gamma', \exists x. A, B \vdash \Delta'} C} \exists_g \quad x \notin FV(\Gamma, \Delta) \\ \vdots & & \vdots \end{array}$$

Enfin, si l'affaiblissement et la règle de quantificateur n'ont pas lieu du même côté, on peut les commuter sans risque.

3. Tout comme pour le système additif, on peut intégrer les affaiblissements aux axiomes dans le système réversible. On peut même intégrer les affaiblissements sur les formules quantifiées aux axiomes et leur faire traverser la partie réversible.

### ► Exercice 3

1.  $\models \exists \vec{x}. F(\vec{x}) \iff \models \neg\neg(\exists \vec{x}. F(\vec{x})) \iff \not\models \neg(\exists \vec{x}. F(\vec{x})) \iff \not\models \forall \vec{x}. \neg F(\vec{x}) \iff \not\models U$
2.  $\models F(t_1) \vee \dots \vee F(t_n) \iff \models \neg\neg(F(t_1) \vee \dots \vee F(t_n)) \iff \not\models \neg(F(t_1) \vee \dots \vee F(t_n)) \iff \not\models \neg F(t_1) \wedge \dots \wedge \neg F(t_n)$
3. Prenons une interprétation  $\mathcal{I}$ . Par contraposition, on montre que  $\mathcal{I} \models U$  entraîne  $\mathcal{I} \models \neg F(t_1) \wedge \dots \wedge \neg F(t_n)$ . Or  $\mathcal{I} \models U$  est par définition  $\mathcal{I} \models \neg F(v)$  pour tout point  $v$ . En particulier pour  $v = t_i$ , on a  $\mathcal{I} \models \neg F(t_i)$ . La définition de la validité pour la conjonction permet de conclure.

► **Exercice 4**

1. La base de Herbrand est dénombrable car le langage l'est.
2. Une branche infinie correspond à une interprétation : il suffit de voir les deux sous-arbres partant d'un nœud interne comme les valeurs attribuées à l'atome qui étiquette le nœud. Avec l'énumération des atomes, on est sûr d'atteindre tous les atomes donc une branche infinie est bien une interprétation. De plus, cette correspondance est une bijection.
3. Une branche est une interprétation. D'après la prémisse du théorème de Herbrand, cette interprétation ne valide pas  $U$ . Par compacité, cette contradiction peut s'obtenir avec un nombre fini d'atomes. Ainsi, on peut couper la branche après l'apparition du dernier atomes et la feuille ainsi créée contient bien une contradiction.
4. On vient de montrer que chaque branche de cet arbre est finie. D'après lemme de König faible, l'arbre est donc fini.

► **Exercice 5**

1. On le vérifie par induction sur la structure de l'arbre en utilisant les équations suivantes :

$$\text{subHtree } p(\text{Leaf } \vec{x}) = \text{eval } p F'(\vec{x}) \quad (1)$$

$$\text{subHtree } p(\text{Node } a t_1 t_2) = \text{subHtree } (p \cup \{a \mapsto \text{true}\}) t_1 \ \&\& \ \text{subHtree } (p \cup \{a \mapsto \text{false}\}) t_2 \quad (2)$$

Cela revient à définir une fonction récursive `subHtree` qui vérifie les équations ci-dessus. Être un arbre de Herbrand revient alors à vérifier `subHtree`  $\emptyset$ .

2. L'énoncé que l'on veut montrer est  $\not\models U \rightarrow \exists t. \text{subHtree } \emptyset t = \text{true}$ . Sa contraposée est donc

$$(\forall t. \text{subHtree } \emptyset t = \text{false}) \rightarrow \exists \rho. \rho \models U .$$

3. Soit  $p$  une valuation finie qui ne possède pas de sous-arbre de Herbrand. Supposons par l'absurde que  $p \cup \{a \mapsto \text{true}\}$  et  $p \cup \{a \mapsto \text{false}\}$  possède chacun un arbre de Herbrand, respectivement  $t_1$  et  $t_2$ . Alors `Node`  $a t_1 t_2$  serait un arbre de Herbrand pour  $p$ , ce qui est absurde. En effet, d'après l'équation (2), on a :

$$\begin{aligned} & \text{Node } a t_1 t_2 \text{ sous-arbre de Herbrand pour } p \\ \iff & \text{subHtree } p(\text{Node } a t_1 t_2) = \text{true} \\ \stackrel{(2)}{\iff} & \text{subHtree } (p \cup \{a \mapsto \text{true}\}) t_1 \ \&\& \ \text{subHtree } (p \cup \{a \mapsto \text{false}\}) t_2 \end{aligned}$$

4. La question précédente nous dit que si  $p$  n'a pas de sous-arbre de Herbrand, on peut l'étendre avec un atome  $a \notin p$  de sorte que le résultat ne possède pas non plus de sous-arbre de Herbrand.

En partant de la valuation vide  $p_0 = \emptyset$ , on itère ce procédé et on construit une suite de valuations finies  $(p_n)_{n \in \mathbb{N}}$  croissante pour l'inclusion. Pour être sûr d'obtenir une interprétation, on choisit à l'étape  $n$  le plus petit atome pas encore dans  $p_{n-1}$  (c'est-à-dire le  $n^{\text{e}}$  atome). Ainsi, chaque atome apparaît dans la suite à un moment et la réunion de cette suite (bien définie car elle est croissante) est une interprétation.

5. Pour montrer que cette interprétation  $\rho_\infty$  est un modèle, il faut montrer qu'elle valide  $U$ . Prenons donc  $\vec{v}$  et montrons que  $\rho_\infty \models F'(\vec{v})$ . Puisque  $\rho_\infty$  est une interprétation, elle contient tous les atomes présents dans  $F'(\vec{v})$ . Par définition de  $\rho_\infty$  comme réunion de la suite  $(p_n)_{n \in \mathbb{N}}$ , cela signifie qu'il existe  $i_\infty$  tel que  $p_{i_\infty}$  contienne tous les atomes présents dans  $F'(\vec{v})$ . Ainsi,  $p_{i_\infty}$  est suffisant pour évaluer  $F'(\vec{v})$ . Si cette valeur était *false*, cela impliquerait que l'arbre `Leaf`  $\vec{v}$  serait un sous-arbre de Herbrand pour  $p_{i_\infty}$  d'après l'équation (1). C'est absurde puisque par construction aucun des  $p_j$  ne possède de sous-arbre de Herbrand. Ainsi la valeur ne peut être que *true* et on en déduit  $\rho_\infty \models F'(\vec{v})$ .