RAIRO. INFORMATIQUE THÉORIQUE

LUIS FARIÑAS DEL CERRO

Un principe de résolution en logique modale

RAIRO. Informatique théorique, tome 18, nº 2 (1984), p. 161-170
<http://www.numdam.org/item?id=ITA_1984__18_2_161_0>

© AFCET, 1984, tous droits réservés.

L'accès aux archives de la revue « RAIRO. Informatique théorique » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme Numérisation de documents anciens mathématiques
http://www.numdam.org/

R.A.I.R.O. Informatique théorique/Theoretical Informatics
(vol. 18, n° 2, 1984, p. 161 à 170).

UN PRINCIPE DE RÉSOLUTION EN LOGIQUE MODALE (*)

par Luis FARIÑAS DEL CERRO (1)

Communiqué par E. ENGELER

Résumé. — *Les applications de la logique modale sont liées aux raisonnements sur les programmes. C'est pour cette raison que nous nous sommes intéressés aux développements de systèmes de démonstration de théorèmes en logique modale. Un système de démonstration de théorèmes de type résolution est présenté. Nous prouvons les deux versions de la propriété de Herbrand, ainsi que la complétude du système.*

Abstract. — *The applications of modal logic are connected with programming reasoning and for this reason we are interested in developping theorem proving system for it. A resolution-style theorem proving system for modal logic is presented. The two version of Herbrand property are proved. The completeness of the system is given.*

Nous présentons dans cet article une formalisation des modalités *de re parfaite de* $S\,5^*$ quantificationnelle [1], [7]. Par modalités *de re parfaite*, nous entendons soit les formules où les variables, dans le champ de leurs opérateurs modaux, sont libres, soit les formules sans opérateurs modaux.

Les applications de la logique modale sont liées à la représentation des connaissances et au raisonnement sur les programmes [5], c'est pour cette raison que nous nous sommes intéressés au développement de démonstrateurs de théorèmes dans de telles logiques.

Nous présentons les deux versions de la propriété de Herbrand, Sur cette base nous développons un système de démonstration de théorèmes de type résolution.

(*) Reçu en décembre 1980, révisé en octobre 1983.

(1) Langages et systèmes informatiques, Université Paul-Sabatier, 118, route de Narbonne, 31062 Toulouse Cedex.

0399-0540/84/02 161 10/$ 3.00/ © AFCET-Bordas

1. PRÉLIMINAIRES

La formalisation que nous adoptons pour $S\,5^*$ avec des quantifieurs ayant la formule de Barcan et son contraire comme théorèmes $(\exists x\, MA(x) \leftrightarrow M \exists x\, A(x))$ [4] est une extension de toute formalisation adéquate du calcul de prédicats classique. Les formules atomiques et leur négation sont appelées littéraux, les symboles A, B, C... représentent des formules arbitraires, $A(x)$ la formule A ayant x comme variable libre, L et M les opérateurs modaux, nécessaire et possible respectivement, LA est défini comme $\sim M \sim A$.

Nous appellerons $S\,5^*$ [3] le système obtenu par adjonction au calcul de prédicats du premier ordre des axiomes et de la règle d'inférence suivante :

A_1. $LA \rightarrow A$

A_2. $\sim LA \rightarrow L \sim LA$

A_3. $L(A \rightarrow B) . \rightarrow . LA \rightarrow LB$

R_1. $\vdash A$, $\vdash LA$.

Une formule est appelée ouverte, si elle ne possède pas de quantificateurs. Nous appellerons modèle de $S\,5^*$ un quadruple ordonné (G, O, D, φ), où O (situations) et D (domaine) sont deux ensembles non vides, et $G \in O$. L'interprétation φ d'une formule A dans la situation $J \in O$ notée $\varphi(A, J)$ est définie, comme usuelle, par induction sur le nombre de symboles logiques de A. Et $\varphi(LB, J) = vraie$ si et seulement si $\varphi(B, J') = vraie$ pour tout $J' \in O$.

Nous dirons que A est vraie dans $R = (G, K, D, \varphi)$ si et seulement si $\varphi(A, G) = vraie$ et A sera valide si elle est vraie dans tous ces modèles.

1.1. Les concepts modaux Nécessaire (L), Contingent positif (CP), Contingent négative (CN) et Impossible (I) sont appelés modalités premières, et sont ainsi définis :

$$CPA =_{\text{def}} A \,\&\, \sim LA \quad CNA =_{\text{def}} \sim A \,\&\, MA \quad IA =_{\text{def}} \sim MA$$

1.2. Forme normale de formules ouvertes (FN).

Une formule ouverte de $S\,5^*$ est en FN si elle est une conjonction de disjonction d'éléments ayant une des formes suivantes :

(a) une formule atomique précédée de l'un des concepts L, CP, CN, ou I

(b) une disjonction de littéraux (comprenant au moins un littéral positif) précédée de l'un des concepts L ou CP

(c) une conjonction de formules atomiques précédée de l'un des concepts CN ou I.

L'ensemble des formules de type (*a*) sera noté *ELE*.

1.3. *Pour toute formule de re parfaite de S5*, il existe une formule équivalente en forme prenex dont la matrice est en FN.*

La démonstration est essentiellement celle donnée dans [3] p. 55, mais relative aux modalités premières.

Étant donné une formule *de re parfaite A*, nous pouvons appliquer la méthode de Skolen pour l'élimination des quantificateurs existentiels de forme usuelle [(8) p. 334].

2. ARBRES SÉMANTIQUES

Une formule A est appelée une E-Clause si c'est une conjonction de disjonctions de formules de *ELE*. Étant donné un ensemble de E-Clauses C, $U(C)$ est l'algèbre libre (appelée univers de Herbrand de C) générée par les constantes et les fonctions de C. S'il n'y a pas de constantes dans C, on associe à $U(C)$ une constante arbitraire.

La base de Herbrand $B(C)$ d'un ensemble de E-Clauses C est l'ensemble des instances des formules atomiques p_i apparaissant dans C, obtenu en substituant les variables de p_i par des éléments de $U(C)$. $[C]$ note l'ensemble des instances de C, sur $U(C)$.

2.1. Soit T un arbre muni d'une racine. Soit ES l'ensemble des sommets de T. Nous appelons branche de T un chemin commençant à la racine. Une branche est appelée complète si elle est infinie ou si elle se termine à un sommet pendant.

2.2. Nous appelons sous-arbre T' d'un arbre T un arbre de même racine que T, contenue dans T et qui pour chaque sommet de T' contient soit tous les successeurs soit aucun.

Il existe une correspondance biunivoque entre l'ensemble des sous-arbres de T et l'ensemble des parties de ES contenant au plus un point de chaque branche de T. Étant donné une telle partie ES', le sous-arbre correspondant T' est obtenu en supprimant dans T les successeurs des éléments de ES'.

2.3. Soit C un ensemble de E-Clauses. Soit $B(C)$ la base de Herbrand de C. Nous définissons un arbre sémantique associé à $B(C)$ comme un arbre tel que :

(*a*) A chaque sommet, différent de la racine est associé une formule de $B(C)$ précédée par un des concepts L, CP, CN ou I.

(*b*) Pour chaque sommet non terminal de T, les formules associées à ses successeurs sont Lp_i, CPp_i, CNp_i et Ip_i pour un $p_i \in B(C)$.

2.4. Soit $B(C) = \{p_1, p_2, \ldots\}$ la base de Herbrand d'un ensemble de E-Clauses C. Un arbre sémantique associé à C est appelé complet, si et seulement si chaque ensemble $\Sigma = \{B_1, B_2, \ldots\}$ où B_i est de la forme P_{p_i} et P est une des modalités premières, coïncide avec l'ensemble des formules associées aux sommets d'une branche α de T.

2.5. Étant donné un arbre sémantique complet T, nous associons à chaque branche complète α de T une interprétation (appelée S-interprétation) définie par la fonction $\varphi\{\alpha\}$:

– $\varphi\{\alpha\}(A) =_{\mathrm{def}}$ *vraie* si $A \in \alpha$,

– $\varphi\{\alpha\}(A) =_{\mathrm{def}}$ *fausse* si $A \notin \alpha$,

dont le domaine est l'ensemble des formules associées aux sommets de T.

Par conséquent chaque formule associée à un sommet de l'arbre T est considérée comme une variable propositionnelle. A chaque sous-ensemble de l'ensemble de sommets d'une branche α nous associons une S-interprétation partielle (restriction de $\varphi\{\alpha\}$ à ce sous-ensemble).

2.6. Un sommet N, d'un arbre associé à C, est appelé *sommet-fermeture* s'il est le premier sommet de la branche $\alpha(N)$, (qui termine en N), dont l'interprétation falsifie un élément de $[C]$.

2.7. Nous disons qu'un arbre sémantique est *fermé* si toutes ses branches possèdent un sommet-fermeture.

2.8. *Un ensemble de E-clauses C est insatisfaisable si et seulement si C est faux pour toutes les S-interprétations (pour chaque arbre sémantique complet).*

La démonstration découle du fait que tout modèle R entraîne trivialement une interprétation en termes de valeurs de vérité sur les formules de *ELE* apparaissant en C.

3. PROPRIÉTÉ DE HERBRAND

3.1. *Un ensemble de E-clauses C est insatisfaisable si et seulement si chaque arbre sémantique pour C contient un sous-arbre fini et fermé.*

Démonstration : (*a*) Soit T l'arbre sémantique complet associé à C. Étant donné que C est insatisfaisable pour chaque branche α de T, il existe un élément de C qui est faux dans la S-interprétation associée à α. Il doit exister un sommet-fermeture puisqu'il existe un nombre fini d'éléments dans chaque clause. Alors le sous arbre T' obtenu par suppression, dans chaque branche, de tous les successeurs du sommet-fermeture de cette branche est fermé et fini par le lemme de König.

(*b*) Supposons que chaque arbre sémantique complet possède un sous arbre fermé fini. Alors pour chaque S-interprétation C sera faux. Donc C est insatisfaisable.

3.2. *Un ensemble de E-Clauses C est insatisfaisable si et seulement s'il existe un ensemble fini d'éléments de* [*C*] *qui est insatisfaisable.*

Démonstration : Il suffit de prendre un ensemble fini quelconque d'éléments de $[C]$ tel que pour chaque sommet-fermeture de T' (3.1) au moins l'un d'entre eux soit falsifié.

4. UNIFICATION

Soit $p=\{p_1, \ldots, p_n\}$ un ensemble de formules atomiques (ou de termes) apparaissant dans les formules de *ELE*. Une substitution s est appelée un unifieur de l'ensemble p si pour tout $i, j=1, \ldots, n$ $p_i s=p_j s$. Un unifieur s est appelé *l'unifieur le plus simple* de l'ensemble A si pour tout unifieur s_2, il existe une substitution s_3 telle que $s_1=s_2 \circ s_3$. Le problème pour trouver l'unifieur le plus simple pour un ensemble d'expression p est décidable [8].

5. LE PRINCIPE DE RÉSOLUTION

La formule atomique d'une formule A de *ELE* sera notée $|A|$. mod (A) est la modalité première de A.

Soit $E_1 \vee A_1$ et $E_2 \vee A_2$, deux E-clauses sans variables communes où A_1 et A_2 sont des formules de *ELE*. Nous introduisons les règles suivantes :

$$\textit{règle de résolution} \quad \frac{E_1 \vee A_1,\ E_2 \vee A_2}{E_1 s \vee E_2 s}$$

où s est l'unifieur le plus simple de l'ensemble $\{|A_1|, |A_2|\}$. La règle de résolution est applicable quand mod $(A_1) \neq$ mod (A_2) :

$$\textit{règle de factorisation} \quad \frac{E_1 \vee A_1 \vee A_2}{E_1 s \vee A_2 s}$$

où s est l'unifieur le plus simple de l'ensemble $\{|\mathrm{A}_1|, |\mathrm{A}_2|\}$. La règle de factorisation est applicable quand $\mathrm{mod}(A_1) = \mathrm{mod}(A_2)$.

5.1. Soit C un ensemble fini de E-clauses, une *déduction* de E à partir de C est une suite finie de E-clauses $E_1, \ldots, E_n$ telle que :

1° : E_n est E;

2° E_i $1 \leqq i \leqq n$ est :

(*a*) un élément de C ou,

(*b*) un facteur de E_j $j < i$ ou,

(*c*) une résolvante de E_j et E_k pour j, $k < i$.

5.2. Une *réfutation* de C est une déduction de la clause vide à partir de C.

Exemple 1 : Soit l'ensemble de E-clauses (insatisfaisables) suivant :

(1) $Lp \vee CPp$,

(2) $CNp \vee Ip$;

par résolution et factorisation, nous obtenons successivement :

(3) $CPp \vee Ip$ utilisant (1) et (2);

(4) $Ip \vee Ip$ utilisant (3) et (2);

(5) Ip par factorisation;

(6) CPp utilisant (5) et (1);

par résolution sur (5) et (6), nous obtenons la clause vide.

Exemple 2 : Soit l'ensemble de E-clauses (insatisfaisables) suivant :

(1) $Lp \vee CPp$;

(2) $CPp \vee CNp$;

(3) $\mathrm{L}p \vee CNp$;

par résolution et factorisation, nous obtenons successivement :

(4) CPp utilisant (1) et (2) et factorisation;

(5) CNp utilisant (4) et (3);

par résolution sur (4) et (5), nous obtenons la clause vide.

5.3. *Soit E'_1 et E'_2 deux instances des E-clauses E_1 et E_2 sans variables communes. Si E'_3 est la résolvante de E'_1 et E'_2, il existe une résolvante E_3 de E_1 et E_2 telle que E'_3 est une instance de E_3.*

La démonstration est essentiellement la même que dans Robinson [8].

5.4. *Si les E-clauses E_1 et E_2 sont satisfaisables et possèdent une résolvante, alors cette résolvante est satisfaisable.*

Démonstration : Soit $E_1 = E_{10} \vee A_1$ et $E_2 = E_{20} \vee A_2$ et R un modèle pour E_1 et E_2, soit $E_{10} \vee E_{20}$ la résolvante de E_1 et E_2. Puisque A_1 *et* A_2 sont (S 5) inconsistantes, A_1, A_2 ou A_1 *et* A_2 sont fausses dans R. Par conséquent, $E_1 \vee E_2$ doit être vraie dans R.

5.5. *Un ensemble C de E-clauses est insatisfaisable si et seulement si il existe une réfutation à partir de C.*

Démonstration :

a. Supposons que C est insatisfaisable.

Soit $\Sigma = \{ |A_1|, |A_2| \ldots \}$ la base associée.

Soit T l'arbre sémantique associé [2]. Par 3.2, nous obtenons un sous arbre T_1 qui est fini et fermé. Supposons que T_1 possède plus d'un sommet sinon la démonstration est triviale. Soit $\mathcal{N}$ l'ensemble de sommets dont tous les successeurs immédiats sont des sommets-fermeture, ($\mathcal{N}$ n'est pas vide puisque T_1 est fini) et soit $N \in \mathcal{N}$.

Soit $\{ N_i : i = 1, \ldots, 4 \}$ l'ensemble des successeurs immédiats de N (*fig.* 1).

Il doit exister des instances A'_1 et A'_2 sur $B(C)$ des formules de ELE, telles que pour chaque i $1 \leqq i \leqq 4$ dans l'interprétation $\mathcal{O}\ \{ F(N_i) \}$ associée à la formule $F(N_i)$ dans le sommet N_i, au moins l'une des assertions :

– A'_1 est fausse,

– A'_2 est fausse,

est vraie.

Soit E'_1 et E'_2 deux instances dans C des E-clauses E'_1 et E'_2 telles que $A'_j \in E'_i$ pour $i = 1, 2$,.

Nous distinguons les deux cas suivants :

a. 1. La E-clause E'_1 (resp. E'_2) ne possède pas une formule A'_{j_1} (resp. A'_{j_2}) de ELE vérifiant les conditions suivantes.

(1) $|A'_1| = |A'_{j_1}|$(resp. $|A'_2| = |A'_{j_2}|$

(2) $\mathrm{mod}(A'_1) \neq \mathrm{mod}(A'_{j_1})$ (resp. $\mathrm{mod}\,(A'_2) \neq \mathrm{mod}(A'_{j_2})$

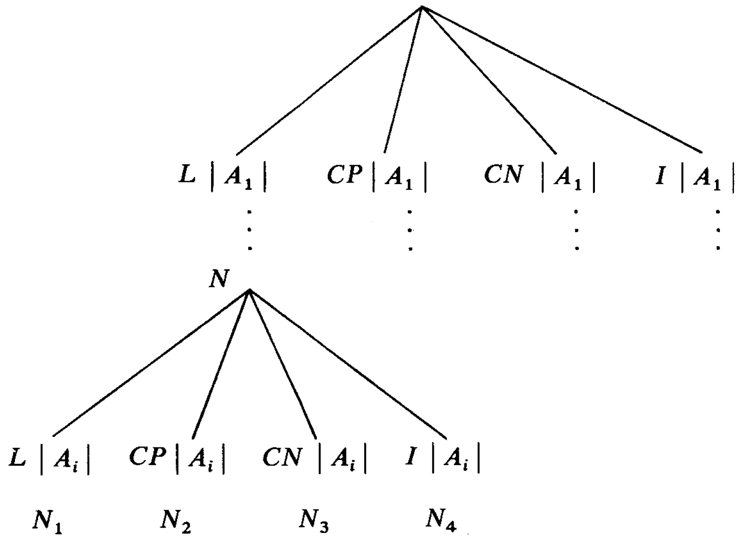

Figure 1

Dans ce cas, pour les interprétations $\varnothing\{\alpha(N_i)\}$ $i=1, 2, 3, 4$,
au moins une des assertions :

– E'_1 est fausse;

– E'_2 est fausse;

est vraie.

Alors par résolution sur A'_1 et A'_2, on obtient la résolvante E' de E'_1 et E'_2 définie par :

$$E' = (E'_1 - A'_1) \vee (E'_2 - A'_2)$$

E' doit être falsifiée dans l'interprétation $\varnothing\{\alpha(N)\}$ puisque $(E'_1 - A'_1)$ et $(E'_2 - A'_2)$ sont falsifiées dans l'interprétation $\varnothing\{\alpha(N)\}$.

$a.2$. S'il existe au moins une formule A'_{j_1} (ou une formule A'_{j_2}) de ELE, telle que $A'_{j_1} \in E'_1$ $(A'_{j_2} \in E'_2)$, vérifiant les conditions (1) et (2) dans a. (Supposant qu'il existe une seule formule A'_{j_1}), nous distinguons les deux sous-cas :

$a.2.1$. Il n'existe pas une formule $A'_j \in \{A_1, A_{j_1}\}$ de ELE telle que $A'_j \in E'_1$ et $A'_j \in E'_2$ (exemple 1 dans 5).

Soit N^1 et N^2, deux sommets successeurs du sommet N, tels que pour les interprétations $\varnothing\{F(N^1)\}$ et $\varnothing\{F(N^2)\}$, A'_1 et A'_2 sont vraies respectivement.

Dans ce cas, pour les interprétations $\mathcal{O}\{\alpha(N_i)\}$ $i=1, 2, 3, 4$ au moins une des assertions :

– E'_1 est fausse;

– E'_2 est fausse;

est vraie.

Alors, par résolution sur A'_1 et A'_2, on obtient la résolvante E' de E'_1 et E'_2, définie par :

$$E'=(E'_1-A'_1) \vee (E'_2-A'_2)$$

E' doit être falsifiée dans les interprétations $\mathcal{O}\{\alpha(N^1)\}$ et $\mathcal{O}\{\alpha(N^2)\}$ puisque $(E'_1-A'_1)$ et $(E'_2-A'_2)$ sont aussi falsifiées dans ces interprétations.

$a.2.2.$ Il existe au moins une formule $A'_j \in \{A_1, A_{j_1}\}$ de ELE (supposant qu'il existe une seule formule) telle que $A'_j \in E'_1$ et $A'_j \in E'_2$ (exemple 2 dans 5).

Soit N_{i_0} le sommet tel que $\mathcal{O}\{F(N_{i_0})\}$ vérifie A'_j. Soit N^1, N^2 deux sommets tels que dans les interprétations $\mathcal{O}\{F(N^1)\}$ et $O\{F(N^2)\}$, A'_1 et A'_2 sont vraies respectivement.

Dans ce cas pour les interprétations $\mathcal{O}\{\alpha(N_i)\}$ $i \in \{\{1, 2, 3, 4\}-i_0\}$ au moins une des assertions :

– E'_1 est fausse;

– E'_2 est fausse;

est vraie.

Alors, par résolution sur A'_1 et A'_2, on obtient la résolvante E' de E'_1 et E'_2, définie par :

$$E'=(E'_1-A'_1) \vee (E'_2-A'_2)$$

E' doit être falsifiée dans l'interprétation $\mathcal{O}\{\alpha(N^1)\}$ et $\mathcal{O}\{\alpha(N^2)\}$ puisque $(E'_1-A'_1)$ et $(E'_2-A'_2)$ sont aussi falsifiées dans ces interprétations.

Par 5.3 il existe une résolvante E de E'_1 et E'_2 telle que E' est une instance de E. Soit T_2 l'arbre sémantique formé, associé à $A \cup \{E\}$, obtenu à partir de T_1 par effacement de chaque sommet ou arête qui suit le premier sommet ou E' est falsifiée.

Dans le cas a, T_2 possède moins de sommets que T_1. Dans le cas $a.2$, T_2 ne possède pas nécessairement moins de sommets que T_1, mais on voit facilement (exemple 1 et 2, dans 5 pour les cas $a.2.1$ et $a.2.2$ respectivement) que nous pouvons nous ramener au cas a, par application successive de l'opération de résolution. Pour le cas $a.2.2$, il faut utiliser une E-clause qui soit fausse pour l'interprétation $\mathcal{O}\{\alpha(N_{i_0})\}$ (exemple 2 dans 5).

Si nous appliquons successivement cette procédure nous obtiendrons l'arbre trivial réduit à la racine, au cas où il existe une réfutation à partir de C.

b. Supposons qu'il existe une réfutation de *C*. Soit $E_1, \ldots, E_n$ ses résolvantes.

Supposons que *C* est satisfaisable. Soit *R* un modèle qui vérifie *C*; par 5.4. *R* doit satisfaire chaque résolvante, en particulier la clause vide, mais ceci est impossible. Alors *C* doit être insatisfaisable.

Exemple 3 : Soit l'ensemble de *E*-clauses insatisfaisables suivant :

(1) $Ip(f(b))$;

(2) $CPq(x) \vee CNr(x)$;

(3) $CNt(y) \vee Ir(y)$,

(4) $CPp(x) \vee It(x)$,

(5) $CNq(f(x))$.

Nous obtenons successivement par résolution :

(6) $It(f(b))$ à partir de (1) et (4).

(7) $CPq(x) \vee CNt(x)$ à partir de (2) et (3);

(8) $CNt(f(x))$ à partir de (5) et (7);

(9) la clause vide à partir de (6) et (8).

BIBLIOGRAPHIE

1. R. Carnap, *Modalities and Quantification*, J.S.L., vol. 11, 1946, p. 33-64.
2. C. Chang et R. Lee, *Symbolic Logic and Mechanical Theorems proving*, Academic Press, 1973.
3. G. Hugues et M. Cresswell, An Introduction to Modal Logic, Methuen and co td, 1972.
4. R. B. Marcus, *A functional Calculus of First Order Based on Strict Implications*, J.S.L., vol. 11, (1946), 1-16.
5. Z. Manna et A. Pnueli, *The modal Logic of Programs N-AIM*-330, Stanford Ail., 1979.
6. J. A. Robinson, *A Machine-Oriented Logic Based on the Resolution Principle*, J.A.C.M., vol. 12, 1965, p. 23-41.
7. P. Tichy, On de Dicto Modalities in Quantified *S*5, *J.* of Philo. Logic 2, 1975, p. 387-392.
8. H. Rasiowa et R. Sikorski, *Mathematics of Metamathematics*, PWN Warszawa, 1963.