MODAL THEOREM PROVING : EQUATIONAL VIEWPOINT

Yves AUFFRAY
Societe des avions M. Dassault
78 quai Marcel Dassault
92210 Saint-Cloud - France

Patrice ENJALBERT *
Laboratoire d'Informatique
University de Caen
14032 Caen Cedex - France

ABSTRACT

We propose a new method for automated theorem proving in first order modal logic. Essentially, the method consists in a translation of modal logic into a specially designed typed first order logic called Path Logic, such that classical modal systems (first order Q, T, 04, S4, S5) can be characterized by sets of equations. The question of modal theorem proving then amounts to classical theorem proving in some equational theories. Different methods can be investigated and in this paper we consider Resolution. We may use Resolution with Paramodulation, or a combination of Resolution and Rewriting techniques. In both cases, known results provide "free of charge" a framework immediately applicable to Path Logic, with completeness theorems. Considering efficiency, the Rewriting method seems better and we present here in details its application to Path Logic. In particular we show how it is possible to define a special kind of skolemisation and design a unification algorithm which insures that two clauses will always have a finite set of resolvents.

INTRODUCTION

In the so-called possible worlds semantics for Modal Logic, modal operators are interpreted as quantifications over "worlds", constrained by some "accessibility" relation. But in the language of modal logic, worlds are not explicitely named, i.e. there is no syntactic item, such as variables or constants, denoting them. We consider that much of the success of Modal Logic comes from this feature, since the variableless operatorsoand o can be closely related with current language operators like "necessary", "always", or "I believe that". But from a theorem proving point of view, is this choice appropriate ? This is not that obvious : just observe the difficulties encountered by different authors who tried to extend Robinson's Resolution method to first order modal theorem proving [Cialdea 86] [Abadi Manna 86] [Konolidge 86]. Indeed it is certainly not easy to cope with the dependencies between objects of the discourse domain and worlds, which are in fact specified by a first order modal formula, in a formalism which avoids naming the latter.

*This work has been partially supported by the GRECO-PRC "Programmation"

A well-known way of restoring, say, a syntactic status to the worlds and the accessibility relation is to translate modal formulas into a first order classical logic with a binary relation symbol to denote the accessibility relation. This direction has been proposed by several authors in the A.I. field (f.i. [Moore 80]). But it seems that we loose much of the structure of the initially given modal formulas in the process of translation, and this is to be paid in terms of efficiency.

In this paper we propose another method for modal theorem proving. This method is based on a translation into a first order classical logic, but the target logic is tailored to better fit the structure of modal formulas.

We call this logic Path Logic. It possesses three types A, W and I). Objects of type I) are those of the discourse domain. Objects of type W represent worlds. Concerning *A,* we can see it as the type of operators on objects of type W. The idea is to capture the notion of accessibility relation in the following way : "the world w^f is accessible from w" will be expressed by the sentence "w* is obtained from w by application of an operator in A". Through our translation in Path Logic, the various systems of modal logic are mapped into equational theories expressing some constraints on the system of operators. Proposition 1 provides the correspondance for Q, T, Q4, S4 and S5.

The question of modal theorem proving then amounts to classical theorem proving in some equational theories. Different methods can be investigated and in this paper, we consider Resolution.We may use Resolution with Paramodulation like in [Walther 87], or a combination of Resolution and Rewriting techniques like in [Plotkin 72] and [Fages 83]. Both these theories provide "free of charge" a framework immediately applicable to Path Logic with completeness theorems (proposition 3). Considering efficiency, Plotkin-Fages method seems better and we present here in details its application to Path Logic.

In particular, we must face the following problem. The equational theories considered for some modal system (Q4,S4)possess an associative operator, and associative unification in general is known as a difficult question [Fages, Huet 86] [Pecuchet 84]. The difficulty is overcome here by defining a special skolemisation ("strong skolemisation"in the paper). A unification algorithm based on these results has been defined and proved correct (proposition 5).

Similar approaches are proposed by L. Farinas and

A. Herzig [Farinas Herzig 88], and H.J. Ohlbach [Ohlbach 88] from who we have borrowed the statement of the Unique Prefix Property. Compared to these papers, ours is characterized by the systematic developpement of an algebraic-equational point of view. This to our sense gives a cleaner mathematical framework and has the invaluable advantage of discharging of a great deal of mathématical work.

1 PATH LOGIC AND THE TRANSLATION OF FIRST ORDER MODAL LOGIC

1.1 Syntax

We consider the language of modal logic built on a signature Σ consisting of :
- a set G of function symbols of any arity
- a set P of predicate symbols of any arity

with the classical and modal connectives $\wedge, \vee, \neg, \forall, \exists, \Diamond, \Box$, and a set V (x, y, z...). Terms and modal formulas are defined in the usual way.

Given some modal system S among Q, T, Q4, S4, S5 L(S) will denote the Path Logic associated with S. As earlier mentionned, L(S) possesses three types $\underline{A}$, $\underline{W}$, $\underline{D}$. Its language is the classical typed first order language built on one of the following signatures Σ_S, according to the modal system S in view. For any term t and type $\underline{T}$, we note "t:T" for "t of type T".

Σ_Q : $\varepsilon : \underline{W}$, constant
$! : \underline{W} \times \underline{A} \rightarrow \underline{W}$, function symbol - for which we use infix notation
The set G of Σ - a function symbol g in G has type $\underline{D}^n \rightarrow \underline{D}$ in Σ_Q if g had arity n in Σ.
The set P of Σ-a predicate symbol p in P has type $\underline{W} \times \underline{D}^n \rightarrow \{0,1\}$ in Σ_Q if p had arity n in Σ.

$\Sigma_T : \Sigma_Q \cup \{1 : \underline{A}\}$

$\Sigma_{Q4} : \Sigma_Q \cup \{* : \underline{A} \times \underline{A} \rightarrow \underline{A}\}$ - again, we use infix notation

$\Sigma_{S4} : \Sigma_{Q4} \cup \Sigma_T$

$\Sigma_{S5} : \Sigma_{S4} \cup \{()^{-1} : \underline{A} \rightarrow \underline{A}\}$

Let Ω (= $\{\alpha, \beta, \gamma, \ldots\}$) a set of variables of type $\underline{A}$. V is the set of variables of type $\underline{D}$. We have the usual notions of well typed terms and formulas. Remark that there is no variables of type $\underline{W}$, so that the only terms possessing this type are ε and $\varepsilon!a_1!\ldots!a_k$, with $a_i : \underline{A}$. The reader can fruitfully interpret such objects as paths in a Kripke structure, where "transitions" from one world to another would be named by some a_j.

1.2. Semantics

The semantics of modal logic considered in this paper is a semantics with constant domains and rigid function symbols. The restriction to rigid function symbols is inessential and only for sake of simplicity : all results in this paper easily extend to flexible symbols. We shall say that a modal formula is S-satisfiable if it admits a model which fulfils the requirements on interpretations for the modal system S.

An interpretation K for L(S) is a classical interpretation, defined by giving a domain for each type $\underline{A}$, $\underline{W}$ and $\underline{D}$, and, for any symbol in Σ_S a function or predicate with the correct type. Moreover we suppose that K satisfies the following equational theory E(S), according to the modal system S in view :

$E(Q) = \emptyset$
$E(T) = \{w ! (a * a') = w ! a ! a',\ (a * a') * a'' = a * (a' * a'')\}$
$E(S4) = E(Q4) \cup E(T) \cup \{a * 1 = a,\ 1 * a : a\}$
$E(S5) = E(S4) \cup \{a * a^{-1} = 1\}$

We say that K is an E(S)-interpretation. The notions of truth, validity, satisfiability are defined in the usual way. We shall say that a formula is L(S)-satisfiable if it admits an E(S)-interpretation.

The idea is the following. Let K be some interpretation and A and W be the domains for type $\underline{A}$ and $\underline{W}$ respectively. W can be considered as a set of worlds and A as a set of operators on W. The sentence "the world w' is accessible from w" is interpreted in Path Logic as "there is an operation a in A such that w' = w! a is true in K". The set of equations E(S) is what corresponds in the Path Logic L(S) to the properties of the accessibility relation for S. For instance reflexivity is expressed by the existence of a neutral element 1 ; transitivity by the existence of an associative operation * on A, such that (A,*) is a semi-group operating on W, or a monoid or a group according to whether we are in L(Q4), L(S4) or L(S5).

If the above equations are oriented from left to right, each set E(S) becomes a rewriting system which can be completed into a canonical one, let's call it R(S) (for the notion of canonical rewriting system, see f.i. [Huet, Oppen 80]). If follows that any term t admits a normal form for R(S).

Given any modal system S (among those under consideration) the Path Logic L(S) consists of the above defined first order language on the signature Σ_S, together with the equational theory E(S)

1.3. Translation from modal logic to path logic

For any term $\pi : W$ and modal formula B, the formula $t(\pi, B)$ is defined by induction on the structure of B :

$t(\pi, p(t_1,\ldots,t_n)) = p(\pi, t_1,\ldots,t_n)$ if p is a predicate symbol

$t(\pi, \neg B) = \neg t(\pi, B)$

$t(\pi, B_1 \Delta B_2) = t(\pi, B_1) \Delta t(\pi, B_2) \quad (\Delta \in \{\wedge, \vee\})$

$t(\pi, \forall x\, B) = \forall x\, t(\pi, B)$

$t(\pi, \exists x\, B) = \exists x\, t(\pi, B)$

$t(\pi, \Box B) = \forall \alpha\, t(\pi ! \alpha, B)$

$t(\pi, \Diamond B) = \exists \alpha\, t(\pi ! \alpha, B)$

$t(\pi, B)$ can be read as "the translation of B with starting point the world denoted by π". The translation of B is $T(B) = t(\varepsilon, B)$

Proposition 1 :

A modal formula B is S-satisfiable iff T(B) is L(S) satisfiable.

Example 1 :
Let $G = \Box \exists x \Box\Diamond p(x)$

$T(G) = \exists \alpha \exists x \forall \beta \exists \gamma\ p(\varepsilon ! \alpha ! \beta ! \gamma, x)$

2* RESOLUTION FOR PATH LOGIC

A Path Logic L(S) is a typed first order equational theory. We can apply Resolution with Paramodulation : for instance, the techniques presented in [Walther 87] immediately apply. Or we can use a combination of Resolution and Rewriting techniques,j and this is what we present now.

2.1 Resolution in equational theories

We first recall that the equational theories E(S) above are defined by canonical rewriting systems. [Plotking 72],[Fages 83] extend Robinson Resolution Principle to this framework in the following way. Let E be some equational theory and $\{t_1,...,t_k\}$ a set of terms ; a E-unifier of $\{t_1,...,t_k\}$ is a substitution $\sigma t_1 =_E \sigma t_2 = ... =_E \sigma t_k$. If E is défined by a canonical rewriting system R_E then $=_E$ is decidable and $t =_E t'$ iff the normal form of t according to R_E is identical to that of t'.

E-resolvant :

Let $C = A_1 \vee ... \vee A_k \vee ... \vee A_n \vee \neg B_1 \vee ... \vee \neg B_m$ and $C' = A'_1 \vee ... \vee A'_n \vee \neg B'_1 \vee ... \vee \neg B'_k \vee ... \vee \neg B'_m$, be two clauses and σ an E-unifier of $\{A_1,..., A_k, B'_1,...,B'_k\}$

$\sigma (A_{k+1} \vee ... \vee A_n \vee A'_1 \vee ... \vee A'_n \vee \neg B_1 \vee ... \vee \neg B_m \vee \neg B'_{k+1} \vee ... \vee \neg B'_m)$ is an E-resolvant of C and C',

Let us call E-resolution the deductive system consisting of one inference rule which, given two clauses C_1 and C_2 allows to infer any E-resolvant of C_1. and C_2. As usual a refutation is a proof of the empty clause.

Theorem 2 (Plotkin, Fages) :
A clausal formula is E-unsatisfiable iff there exists a refutation of this formula by E-resolution,

Let us apply this result to Path Logic, We can introduce in the signature S skolem functions of the convenient arities and types and associate, in the standard way, with every formula H of L(S) a clausal formula H' equivalent to H with respect to L(S)-satisfiability. Combining this process with the traduction T thanks to proposition 1, we can associate with every modal formula B of S a formula B' of L(S) in clausal form such that B' is L(S)-unsatisfiable iff B is S-unsatisfiable. Then we have :

Proposition 3 :

Let B any modal formula, S any system among Q, T, Q4, S4, S5, and B' the skolemized of T(B). B is S-unsatisfiable iff we can refute B' by E(S)-resolution.

Example 2 : S5-validity of $\Diamond p \rightarrow \Box\Diamond p$:

We prove the S5-unsatisfiability of $F = \Diamond p \wedge \Diamond\Box \neg p$

Translation : $T(F) = \exists\alpha\ p(\varepsilon ! \alpha) \wedge \exists\beta \forall\gamma \neg p(\varepsilon ! \beta ! \gamma)$

Skolemization : $p(\varepsilon ! \varphi_0) \wedge \forall\gamma \neg p(\varepsilon ! \varphi_1 ! \gamma)$

Clausal form : $C_1 = p(\varepsilon ! \varphi_0)$

$C_2 = \neg p(\varepsilon ! \varphi_1 ! \gamma)$

Resolvant of C_1 and C_2:

let σ be defined by : $\sigma\gamma = \varphi_1^{-1} * \varphi_0$.

σ is an E(S5)-unifer of $p(\varepsilon ! \varphi_0)$ and $p(\varepsilon ! \varphi_1 ! \gamma)$: $\sigma(\varepsilon ! \varphi_0) = \varepsilon ! \varphi_0$ and $\sigma(\varepsilon ! \varphi_1 ! \gamma) = \varepsilon ! \varphi_1 ! (\varphi_1^{-1} * \varphi_0) =_{E(S5)} \varepsilon ! \varphi_0$

Thus, the empty clause is a resolvant of C_1 and C_2

2.2 Strong skolemisation

We recall some definitions. Given some set T of terms, a Complete Set of Unifiers (CSU) for T is a set S of unifiers of T such that for any unifier a of T, there is some T in S such that T is more general than a : there is some u such that $0 = T\ U$.

In order to automatise the search for refutations of sets of clauses, it is quite desirable (but not strictly necessary) to be sure that any unifiable family $\{t_1, ...,tk,\}$ of terms admits a finite CSU. In the empty theory, f.i. E(Q), we know that such sets exist and are in fact reduced to singletons (most general unifiers), and we know algorithms to produce them. It is easy to check that there also exist finite CSU's in the case of E(T), and to exhibit a unification procedure. But in E(Q4), E(S4) or E(S5) we have an associativity axiom for *, and complete sets of unifiers are in general infinite.

Counter example 3 :
Let $E = E(Q4) = \{w ! (\alpha * \alpha') = w ! \alpha ! \alpha',\ (\alpha * \alpha') * \alpha'' = \alpha * (\alpha * \alpha'')\}$. The E-unifiers of $\{\varepsilon ! \alpha ! a, \varepsilon ! a ! \alpha\}$ are

$\theta_1 : \alpha \dashrightarrow a$

...

$\theta_n : \alpha \dashrightarrow a*a*...*a$

...

there is no finite complete set of E-unifiers.

It is possible to enumerate the members of a complete set of unifiers, f.i. using the "narrowing" procedure [Fages 83] [Fay 79]. But there is a better way on. We can take advantage of the particular structure of the formulas obtained in L(S) by trans lation from S, and perform a skolemisation finer than the standard one, which will ensure the desirable finiteness property. This is what we call strong skolemisation. At the present time it is defined for the modal systems Q, T, Q4, S4, so that they are the only systems under consideration in this section.

Since the process of strong skolemisation is a bit complex, we rather present here the result T"(B) of applying it to the translation T(B) of a modal formula B.

Let B a modal formula in negative normal form (negation operating on a atomic formulas).
$T'(B) = t'(\varepsilon, \emptyset, B)$ where, if π is of type $\underline{W}$ and X is a set of $\underline{D}$-typed variables, $t'(\pi,X,B)$ is recursively defined by :

$t'(\pi,X, p(t_1,\cdots,t_n)) = p(\pi,t_1,\cdots,t_n)$

if p is a predicate symbol

$t'(\pi,X, \neg p(t_1,\cdots,t_n)) = \neg p(\pi,t_1,\cdots,t_n)$

if p is a predicate symbol

$t'(\pi,X, B_1 \Delta B_2) = t'(\pi,X, B_1) \Delta t'(\pi,X, B_2)$
$(\Delta \in \{\wedge, \vee\})$

$t'(\pi,X, \forall x\ B) = \forall x\ t'(\pi,X \cup \{x\}, B)$

$t'(\pi,X, \exists x\ B) = t'(\pi, X \cup \{x\}, B)\ [f(\pi,X) / x]$

$f : \underline{W} \times \underline{D}^n \longrightarrow \underline{D}$

$t'(\pi,X, \Box B) = \forall \alpha\ t'(\pi!\alpha, X, B)$

$t'(\pi,X, \Diamond B) = t'(\pi!\varphi(X), X, B)$

$\varphi\ \underline{D}^n \longrightarrow \underline{A}$

Example 4 :

Let $G = \Box\Box\exists x \Diamond p(x)$. We have :
$T(G) = \forall \alpha\forall\beta\ \exists x \exists\gamma\ p(\varepsilon!\alpha!\beta!\gamma, x)$, and the strongly skolemized form is :
$\forall \alpha\forall\beta\ p(\varepsilon!\alpha!\beta!\varphi(\varphi(\varepsilon!\alpha!\beta)), g(\varepsilon!\alpha!\beta))$

As one can see on this example, the general idea is to replace skolem terms depending on $\underline{A}$-variables (such as $f(\alpha,\beta)$), by skolem terms depending on path expressions (like in $g(\varepsilon!\alpha!\beta)$).

Proposition 4 :

Let B be some modal formula and T'(B) the strong skolemisation of T(B). B is satisfiable in S iff T'(B) is satisfiable in L(S).

Skolemised formulas can then be put into clausal form. The clausal formulas obtained that way, possess a property which guarantees that terms to be unified admit a finite complete set of unifiers, namely :

Let C be a clause and $\alpha : \underline{A}$ a variable. For every sub-term $\pi!\alpha : \underline{W}$ in C, π does not depend on the particular occurence of α, but uniquely on α. We call this property the Unique Prefix Property (U.P.P.). In particular it follows that if $\pi!\alpha!a_1!\ldots!a_k : \underline{W}$ is a sub-term of C, α does not occur in π and $a_j \neq \alpha$ for all $j = 1\ldots k$

For example one can easily check that the formula T'(G) in example 3 satisfies this condition, while the set in the counter-example 3 does not.

Proposition 5 : Any set of expressions that satisfies the U.P.P. admits a complete set of E(S)-unifiers. There is a procedure that computes such a set of E(S)-unifiers. The substitutions which are computed preserve the U.P.P. on the given expressions.

It follows from proposition 5 and Plotkin-Fages' results that the classical semi-decision procedure for checking unsatisfiability of a set of clauses can be adapted to Path Logics in a straightforward way. By means of the translation T', we obtain a semi-decision procedure for the modal systems under consideration. The algorithm is given in [Auffray, Enjalbert 88] and proved correct in [Auffray 89].

3. EXTENSIONS - DISCUSSION

Extensions

Our method can be extended to deal with logics with several different modalities (or multimodal logics) such as epistemic logic with many agents. If no relation is specified between the modal operators, we just need to consider subtypes of type A corresponding to the different modal operators, and the characteristic set of equations for each one. We can also deal with relations between modalities specified by axiom schemas like A —D A, by setting some order on the subtypes. Again Walther's techniques immediately apply, and we are studying the extension of Plotkin-Fages ones.

Discussion

1 - The Unique Prefix Property constitutes a characterisation of a subset of the set of formulas of Path Logic in which Modal Logic can be embedded. This feature distinguishes our translation from the "trivial" one envolving a binary relation symbol to denote the accessibility relation. We consider that it indicates that translation from modal logic to path logic is a good compromise keeping part ot the structure of modal formulas while adding what is necessary of extra mathematical structure.

Also in the "trivial" translation, properties of the accessibility relation would be expressed by clauses at the same level than the other ones characterizing the problem to be solved. This situation would be very similar to the treatment of equality which consists in adding a predicate symbol "=" with clauses to express its properties ; this is known to be the wrong way to do . Further on, the use of Rewriting techniques seems likely to give better efficiency than Paramodulation : see [Plotkin 72] for this discussion.

2 - In this paper we considered Resolution, but other classical theorem proving techniques could be used for Path Logic. Fo instance techniques based on rewriting [Hsiang, Dershowitz 83] could be of interest.

3 - A nice feature of our theory is that the treatment of modalities is finally reduced to unifica- in an equational theory. Unfortunately it is likely that not all modal systems can be delt with that way : consider a system like G where the property of the accessibility relation is of topological nature, or some Temporal Logics with the same characteristic. But nothing prohibits to mix the techniques of this paper with other ones, induction for example. This remains to be investigated. Also the question of S_5 must be considered.

On the other hand we can ask which semantical properties can be nicely expressed in the language of Path Logic.

REFERENCES

[Abadi, Manna 86] M. Abadi, Z. Manna. Modal theorem proving, Proc. 8 Internat. Conf. on Automated Deduction : 1986, 172-189

[Auffray 89] Y. Auffray : Resolution Modale et Logique des Chemins, these de 1'Universite de Caen, 1989

[Auffray, Enjalbert 88] Y. Auffray, P. Enjalbert : Modal theorem proving using equational methods : technical Report n° 88-11, Laboratoire d'Informatique, Universite de Caen, 1988

[Cialdea 86] M. Cialdea : Une methode de deduction automatique en logique modale, These de 1'University P. Sabatier, Toulouse, France, 1986.

[Fages, Huet 86] F. Fages, G. Huet : Complete sets of unifiers and matchers in equational theories, Theor. Comput. Scie. : 43, 1986, 189-200

[Fages 83] F. Fages : Formes canoniques dans les algebres booleennes et application a la demonstration automatique en logique du premier ordre. These de 3eme cycle, Paris 7, France, 1983.

[Farinas, Herzig 88] L. Farinas, A. Herzig : Quantified modal logic and unification theory, : Rapport technique LSI n° 293, Universite P. Sabatier, Toulouse, France, 1988.

[Fay 79] M. Fay : First.order unification in equational theories, 4 workshop on automated deduction, Austin, Texas, 1979.

[Hsiang, Dershowitz 83] J. Hsiang, N. Dershowitz, Rewrite methods for clausal and non-clausal theorem proving, Int. Conf. on Automata, Languages and Programming 1983.

[Huet, Oppen 80] G. Huet, D. Oppen : Equations and Rewrite Rules : a survey, in : Formal languages, perspectives and open problems, Book R. ed., Academic Press 1980.

[Konolidge 86] K. Konolidge : A deduction model of belief, Research Notes in Artificial Intelligence, Pitman Pub. Lted, 1986.

[Moore 80]R.C. Moore : Reasoning about knowledge and action, PhD Thesis, MIT, Cambridge, Massachussets, 1980.

[Ohlbach 88] H.J. Ohlbach : A resolution calculus for modal logics, 9^{tn} Conf. on Automated Deduction Springer Lecture Notes in Comput. Scie. 310, 1988, 500-516.

[Pecuchet 84] J.P. Pecuchet : Solutions principales et rang d'un systeme d'equations avec constantes dans le monoide libre, Discrete Mathematics : 48, 1984, 253-274.

[Plotkin 72] G. Plotkin : Building in equational theories, Machine Intelligence 7, 1972, 73-90

[Walther 87] C. Walther : A many-sorted calculus based on resolution and parambdulation Research notes in Artificial Intelligence, Pitman, London, 1987.