Implementing Different Proof Calculi for First-order Modal Logics

– Extended Abstract –

Christoph Benzmüller\(^{1}\)*, Jens Otten\(^{2}\) and Thomas Raths\(^{2}\)†

\(^{1}\) Institut für Informatik, FU Berlin, Germany
c.benzmueller@googlemail.com

\(^{2}\) Institut für Informatik, University of Potsdam, Germany
jeotten|traths@cs.uni-potsdam.de

1 Introduction

Modal logics extend classical logic with the modalities "it is necessarily true that" and "it is possibly true that" represented by the unary operators □ and ◇, respectively. First-order modal logics (FMLs) extend propositional modal logics by domains specifying sets of objects that are associated with each world, and the standard universal and existential quantifiers [7].

FMLs have many applications, e.g., in planning, natural language processing, program verification, querying knowledge bases, and modeling communication. These applications motivate the use of automated theorem proving (ATP) systems for FMLs. Whereas there are some ATP systems available for propositional modal logics, e.g., MSPASS [9] and modleanTAP [1], there were — until recently — no (correct) ATP systems that can deal with the full first-order fragment of modal logics.

This abstract presents several new ATP systems for FML and sketches their calculi and working principles. The abstract also summarizes the results of a recent comparative evaluation of these new provers (see [4] for further details).

The syntax of first-order modal logic adopted here is: 

\[
F, G ::= P(t_1, \ldots, t_n) \mid \neg F \mid F \land G \mid F \lor G \mid F \rightarrow G \mid \Box F \mid \Diamond F \mid \forall x F \mid \exists x F.
\]

The symbols \(P\) are \(n\)-ary (\(n \geq 0\)) relation constants which are applied to terms \(t_1, \ldots, t_n\). The \(t_i\) (\(0 \leq i \leq n\)) are ordinary first-order terms and they may contain function symbols. The usual precedence rules for logical constants are assumed.

Regarding semantics a well accepted and straightforward notion of Kripke style semantics for FML is adopted [7]. In particular, it is assumed that constants and terms are denoting and rigid, i.e. they always pick an object and this pick is the same object in all worlds. Regarding the universe of discourse constant domain, cumulative domain and varying domain semantics are considered.

The following new ATP systems for FML were developed by the authors (partly as extensions of other systems); they support different combinations of modal logics and domain semantics (GQML-Prover [19] has not been included since it returned incorrect results in our experiments for several formulae):

\(^{*}\)This author is funded by the German Research Foundation DFG under reference number BE2501/9-1.

\(^{†}\)This author is funded by the German Research Foundation DFG under reference number KR858/9-1.
2 Calculi and ATP Systems for FML

Sequent Calculus. The classical sequent calculus $LK$ is probably the most elegant calculus for classical logic and used in many interactive proof systems. This calculus can be extended to modal logics with cumulative domains by adding the modal rules $\Box$-left, $\Box$-right, $\Diamond$-left, and $\Diamond$-right. These rules introduce the modal operators $\Box$ and $\Diamond$ into the left side or the right side of the sequent, respectively. All rules of the classical sequent calculus, e.g., the rules for the quantifiers remain unchanged [20].

The sequent calculus for the modal logics K, K4, D, D4, T, and S4 with cumulative domains consists of the axiom and rules of the classical sequent calculus and the four additional rules shown in Figure 1, with

$$\Gamma^+, F \vdash \Delta^+$$ $\Box$-left
$$\Gamma \vdash F, \Delta^*$$

$$\Gamma^*, F \vdash \Delta^*$$ $\Diamond$-right
$$\Gamma, F \vdash \Delta$$

$$\Gamma^+, F \vdash \Delta$$ $\Diamond$-left
$$\Gamma, F \vdash \Delta$$

$$\Gamma^+, F \vdash \Delta$$ $\Diamond$-right
$$\Gamma, F \vdash \Delta$$

Figure 1: The additional modal rules of the modal sequent calculus

The modal sequent calculus captures the cumulative domain condition. There are no similar cut-free sequent calculi for modal logics with constant or varying domains or for the modal logic S5 [20].

MleanSeP is an ATP system written in PROLOG that implements the sequent calculus for several modal logics. It can be downloaded at http://www.leancop.de/mleansep/. MleanSeP performs proof search in an analytic way, i.e. the sequent rules are applied from bottom to top. Furthermore, free-variables are used in combination with a dynamic Skolemization that is calculated during the proof search. Together with the occurs-check of the term unification algorithm this ensures that all derivations respect the Eigenvariable condition. To deal with constant domains, the Barcan formula is automatically added to the given formula in a preprocessing step. The Barcan formula (scheme) has the form $\forall x (\Box P(x)) \Rightarrow \Box \forall x P(x)$ with $x = x_1, \ldots, x_n$ for all predicates $P$ with $n \geq 1$. 

<table>
<thead>
<tr>
<th>ATP system</th>
<th>base technique</th>
<th>modal logics</th>
<th>domain semantics</th>
</tr>
</thead>
<tbody>
<tr>
<td>MleanSeP 1.2</td>
<td>sequent calculus</td>
<td>K,K4,D,D4,T,S4</td>
<td>const.,cumul.</td>
</tr>
<tr>
<td>MleanTAP 1.3</td>
<td>tableau calculus</td>
<td>D,T,S4,S5</td>
<td>const.,cumul.,varying</td>
</tr>
<tr>
<td>MleanCoP 1.2</td>
<td>connection calculus</td>
<td>D,T,S4,S5</td>
<td>const.,cumul.,varying</td>
</tr>
<tr>
<td>f2p-MSPASS 3.0</td>
<td>instance-based method</td>
<td>K,K4,K5,KB,D,T,S4,S5</td>
<td>const.,cumul.</td>
</tr>
<tr>
<td>LEO-II 1.3.2-M1.0</td>
<td>embedding in HOL</td>
<td>K,K4,K5,KB,D,T,S4,S5</td>
<td>const.,cumul.,varying</td>
</tr>
<tr>
<td>Satallax 2.2-M1.0</td>
<td>embedding in HOL</td>
<td>K,K4,K5,KB,D,T,S4,S5</td>
<td>const.,cumul.,varying</td>
</tr>
</tbody>
</table>
Implementing Different Proof Calculi for First-order Modal Logic

C. Benzmüller, J. Otten, T. Raths

prefix characterization for modal logic [20] but uses a tableau-based search to ensure that all paths contain a complementary connection. A prefix is a string consisting of (prefix) variables and (prefix) constants. Essentially, it represents a world path that captures the particular Kripke semantics of the modal logic in question. A prefixed formula has the form $F^{\text{pol}}_p$, where $F$ is a (first-order) modal formula, $\text{pol} \in \{0, 1\}$ is its polarity and $p$ is its prefix.

The (prefixed) tableau calculus for the modal logics D, T, S4, and S5 consists of the rules of the classical tableau calculus [6], which do not change the prefix $p$ of formulae, and the four additional rules shown in Figure 2. $V^*$ is a new prefix variable, $a^*$ is a new prefix constant and $\circ$ is the composition of two strings. A branch is closed if, and only if, it contains a pair of literals of the form $\{A_1^1 : p_1, A_2^1 : p_2\}$ that are complementary under a term substitution $\sigma_Q$ and an additional modal substitution $\sigma_M$, i.e. $\sigma_Q(A_1) = \sigma_Q(A_2)$ and $\sigma_M(p_1) = \sigma_M(p_2)$. A tableau proof for a prefixed formula $F^{\text{pol}}_p$ is a tableau derivation such that all branches are (simultaneously) closed for a pair of term and modal substitutions $(\sigma_Q, \sigma_M)$. A tableau proof for a modal formula $F$ is a tableau proof for $F^{\text{pol}}_p$.

In the prefixed tableau calculus the particular modal logic is specified by distinct properties of the modal substitution $\sigma_M$. An additional admissible criterion on $\sigma_M$ is used to capture the different domain variants, i.e., constant, cumulative, or varying domains.

MleanTAP is a compact ATP system written in PROLOG that implements the modal tableau calculus. In can be downloaded at http://www.leancop.de/mleantap/. The proof search of MleanTAP is split up into two phases. The first phase performs a purely classical proof search. In the second phase, after a classical tableau proof is found, the prefixes $p_1$ and $p_2$ of all literals that close branches in the classical tableau are unified. The unification of these prefixes is done by a specialized string unification algorithm. If the prefix unification fails, alternative classical proofs (and prefixes) are computed. In order to fulfill the distinct properties of the modal substitution $\sigma_M$, a specific unification algorithm is used for each modal logic that also respects the admissible criterion.

### Tableau Calculus

In general, the (classical) tableau calculus can be seen as compact representations of the (classical) sequent calculus. The classical tableau calculus [16] can be extended to several modal logics by adding a prefix to each formula occurring in a tableau rule [6]. The following tableau calculus for modal logic uses free variables not only within terms but also within prefixes. It is based on the matrix characterization for modal logic [20] but uses a tableau-based search to ensure that all paths contain a complementary connection. A prefix is a string consisting of (prefix) variables and (prefix) constants. Essentially, it represents a world path that captures the particular Kripke semantics of the modal logic in question. A prefixed formula has the form $F^{\text{pol}}_p$, where $F$ is a (first-order) modal formula, $\text{pol} \in \{0, 1\}$ is its polarity and $p$ is its prefix.

The (prefixed) tableau calculus for the modal logics D, T, S4, and S5 consists of the rules of the classical tableau calculus [6], which do not change the prefix $p$ of formulae, and the four additional rules shown in Figure 2. $V^*$ is a new prefix variable, $a^*$ is a new prefix constant and $\circ$ is the composition of two strings. A branch is closed if, and only if, it contains a pair of literals of the form $\{A_1^1 : p_1, A_2^1 : p_2\}$ that are complementary under a term substitution $\sigma_Q$ and an additional modal substitution $\sigma_M$, i.e. $\sigma_Q(A_1) = \sigma_Q(A_2)$ and $\sigma_M(p_1) = \sigma_M(p_2)$. A tableau proof for a prefixed formula $F^{\text{pol}}_p$ is a tableau derivation such that all branches are (simultaneously) closed for a pair of term and modal substitutions $(\sigma_Q, \sigma_M)$. A tableau proof for a modal formula $F$ is a tableau proof for $F^{\text{pol}}_p$.

In the prefixed tableau calculus the particular modal logic is specified by distinct properties of the modal substitution $\sigma_M$. An additional admissible criterion on $\sigma_M$ is used to capture the different domain variants, i.e., constant, cumulative, or varying domains.

MleanTAP is a compact ATP system written in PROLOG that implements the modal tableau calculus. In can be downloaded at http://www.leancop.de/mleantap/. The proof search of MleanTAP is split up into two phases. The first phase performs a purely classical proof search. In the second phase, after a classical tableau proof is found, the prefixes $p_1$ and $p_2$ of all literals that close branches in the classical tableau are unified. The unification of these prefixes is done by a specialized string unification algorithm. If the prefix unification fails, alternative classical proofs (and prefixes) are computed. In order to fulfill the distinct properties of the modal substitution $\sigma_M$, a specific unification algorithm is used for each modal logic that also respects the admissible criterion.

### Connection Calculus

Connection calculi use a connection-driven search strategy and are already successfully used for automated theorem proving in classical and intuitionistic logic [11][12]. A connection is a pair of literals, $\{A, \neg A\}$ or $\{A^1, A^0\}$, with the same predicate symbols but different polarities. The connection calculus for classical logic is adapted to modal logic by adding prefixes to all literals. Formally, a prefix is a string over an alphabet $\mathcal{U} \cup \Pi$, where $\mathcal{U}$ is a set of prefix variables, denoted by $V$, and $\Pi$ is a set of prefix constants, denoted by $\alpha$. It is defined in the same way as in the tableau calculus. Subformulae of the form $(\Box F)^1$ or $(\Diamond F)^0$ extend the prefix by a variable $V$, subformulae of the form $(\Box F)^0$ or $(\Diamond F)^1$ extend the prefix by a constant $\alpha$ (see also Figure 2). For the modal logic S5 only the last character of all prefixes is considered (or $\varepsilon$ if the prefix is the empty string $\varepsilon$).

Proof-theoretically, a prefix of a formula $F$ captures the modal context of $F$ and specifies the sequence of modal rules of the sequent calculus that have to be applied (analytically) in order to obtain $F$ in the sequent. Semantically, a prefix denotes a specific world in a model [6][20]. The prefixes of the two literals in a connection, which corresponds to an axiom in the sequent calculus, need to denote...
Implementing Different Proof Calculi for First-order Modal Logic

C. Benzmüller, J. Otten, T. Raths

A connection proof for \( C, M, \text{Path} \) is a derivation such that all leaves are axioms for an admissible substitution \( \sigma = (\sigma_Q, \sigma_M) \). A modal connection proof for the matrix \( M \) is a modal connection proof for \( \varepsilon, M, \varepsilon \). Correctness and completeness proofs are based on the the matrix characterization for modal logic [20] and the correctness and completeness of the connection calculus [5].

\textit{M}eanCoP [13] is an implementation of the modal connection calculus. It can be downloaded at 
http://www.leancop.de/mleancop/. It is based on \textit{leanCoP}, an automated theorem prover for first-order classical logic [11]. To adapt the implementation to the modal connection calculus the \textit{leanCoP} prover is extended by (a) prefixes that are added to literals and collected during the proof search and (b) an additional list that contains term variables together with their prefixes in order to check the domain condition. First, \textit{M}eanCoP performs a classical proof search. After a classical proof is found, the prefixes of the literals in each connection are unified and the domain condition is checked. A different unification algorithm is used for each of the modal logics D, T, S4, and S5. For the modal logic K, the matrix characterization [20] requires to check an additional criterion, which cannot be integrated into the modal connection calculus [13] in a straightforward way. This also applies to the modal tableau calculus presented above. \textit{M}eanCoP uses additional techniques to prune the search space: regularity, lemmata, restricted backtracking, a definition clausal form translation, and a fixed strategy scheduling; see [12] for details.

Figure 3: The modal connection calculus

\[
\begin{align*}
\text{Axiom (A)} & : \quad \{\}, M, \text{Path} \quad \quad \text{Start (S)} & : \quad \varepsilon, M, \varepsilon \quad \text{and } C_2 \text{ is a copy of } C_1 \in M \\
\text{Reduction (R)} & : \quad C, M, \text{Path} \cup \{L_2; p_2\} \quad \quad \text{and } \{L_1; p_1, L_2; p_2\} \text{ is } \sigma\text{-complementary} \\
\text{Extension (E)} & : \quad C_2 \setminus \{L_2; p_2\}, M, \text{Path} \cup \{L_1; p_1\} \quad \quad \text{and } C_2 \text{ is a copy of } C_1 \in M, \\
& \quad \quad \quad \quad L_2; p_2 \in C_2, \text{ and } \{L_1; p_1, L_2; p_2\} \text{ is } \sigma\text{-complementary}
\end{align*}
\]
Embedding into Classical Higher-Order Logic. Various non-classical logics, including FMLs, can be embedded in classical higher-order logic (HOL) \[2, 3\]. The approach exploits the fact that Kripke structures can be elegantly modeled in HOL \[3\]. FML propositions \( F \) are associated with HOL terms \( F_p \) of predicate type \( p : = t \rightarrow o \). Type \( o \) denotes the set of truth values and type \( t \) is associated with the domain of possible worlds. Thus, the application \( (F_p,w_i) \) corresponds to the evaluation of FML proposition \( F \) in world \( w \). Consequently, validity is formalized as \( \text{vld}_{p \rightarrow o} = \lambda F_p \forall w_i F_w \). Classical connectives like \( \neg \) and \( \vee \) are simply lifted to type \( p \) as follows: \( \neg p \rightarrow o = \lambda F_p \forall w_i \neg F_w \) and \( \forall p \rightarrow o = \lambda F_p \exists w_i (F \vee G w) \). \( \exists \) is modeled as \( \square p \rightarrow o = \lambda F_p \forall w_i \forall w_j (\neg Rw_j \vee F v) \), where constant symbol \( R_{i \rightarrow i \rightarrow o} \) denotes the accessibility relation of the \( \square \) operator, which remains unconstrained in logic \( K \). Further logical connectives are defined as usual: \( \wedge = \lambda F_p \lambda G_p \neg(F \vee G) \), \( \Rightarrow = \lambda F_p \lambda G_p (\neg F \vee G) \), \( \exists = \lambda F_p \neg \square \neg F \). To obtain e.g. modal logic S4, \( R \) is axiomatized as reflexive and transitive. Generally, this can be done ‘semantically’ (e.g. with axiom \( \forall x (Rx xx) \) for reflexivity) or ‘syntactically’ (e.g. with axiom \( \text{vld} \forall F_p \square F \Rightarrow F \), where quantification over propositions is employed \[3\]). Arbitrary normal modal logics extending \( K \) can be axiomatized this way. However, in some cases only the semantic approach (e.g. for the irreflexivity of \( R \)) or the syntactic approach (e.g. for McKinsey’s axiom) is applicable.

For individuals a further base type \( \mu \) is reserved in HOL. Universal quantification \( \forall x F \) is introduced as syntactic sugar for \( \Pi \lambda x F \), where \( \Pi \) is defined as follows: \( \Pi (\mu \rightarrow o) = \lambda H_{\mu \rightarrow o} \forall x \forall w_i H x w \). For existential quantification, \( \sum = \lambda H_{\mu \rightarrow o} \Pi \lambda x_i \neg H x \) is introduced. \( \exists x F \) is then syntactic sugar for \( \Sigma \lambda x F \). n-ary relation symbols \( P \), n-ary function symbols \( f \) and individual constants \( c \) in FML obtain types \( \mu_1 \rightarrow \ldots \rightarrow \mu_n \rightarrow o \), \( \mu_1 \rightarrow \ldots \rightarrow \mu_n \rightarrow \mu_{n+1} \) (with \( \mu_i = \mu \) for \( 0 \leq i \leq n + 1 \)) and \( \mu \), respectively.

For any FML formula \( F \) holds: \( F \) is a valid in modal logic \( K \) for constant domain semantics if and only if \( \text{vld} F_p \) is valid in HOL for Henkin semantics. This correspondence provides the foundation for proof automation of FMLs with HOL-ATP systems. The correspondence follows from Benzmüller and Paulson \[3\], who prove a more general result for FMLs with additional quantification over propositional variables. (However, function and constant symbols are avoided in their work to achieve a leaner theory.)

The above approach is adopted for varying domain semantics as follows: 1. \( \Pi \) is now defined as \( \Pi = \lambda H_{\mu \rightarrow o} \forall w_i \forall x \exists w \text{exIn}x w, w \Rightarrow H x w \), where relation \( \text{exIn}w_{\mu \rightarrow o} \) (for ‘exists in world’) relates individuals with worlds. 2. The non-emptiness axiom \( \forall w_i \exists x \text{exIn}x w \forall \text{these individual domains is added.} 3. For each individual constant symbol \( c \) an axiom \( \forall w_i \text{exIn}w c w \) is postulated; these axioms enforce the designation of \( c \) in the individual domain of each world \( w \). Analogous designation axioms are required for function symbols.
Implementing Different Proof Calculi for First-order Modal Logic  
C. Benzmüller, J. Otten, T. Raths

<table>
<thead>
<tr>
<th>Logic</th>
<th>Domain</th>
<th>f2p-MSPASS</th>
<th>MleanSeP</th>
<th>MleanTAP</th>
<th>LEO-II</th>
<th>Satallax</th>
<th>MleanCoP</th>
</tr>
</thead>
<tbody>
<tr>
<td>K</td>
<td>varying</td>
<td>-</td>
<td>-</td>
<td>73</td>
<td>104</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>cumulative</td>
<td>70</td>
<td>121</td>
<td>-</td>
<td>89</td>
<td>122</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>constant</td>
<td>67</td>
<td>124</td>
<td>-</td>
<td>120</td>
<td>146</td>
<td>-</td>
</tr>
<tr>
<td>D</td>
<td>varying</td>
<td>-</td>
<td>-</td>
<td>100</td>
<td>81</td>
<td>113</td>
<td>179</td>
</tr>
<tr>
<td></td>
<td>cumulative</td>
<td>79</td>
<td>130</td>
<td>120</td>
<td>100</td>
<td>133</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td>constant</td>
<td>76</td>
<td>134</td>
<td>135</td>
<td>135</td>
<td>160</td>
<td>217</td>
</tr>
<tr>
<td>T</td>
<td>varying</td>
<td>-</td>
<td>-</td>
<td>138</td>
<td>120</td>
<td>170</td>
<td>224</td>
</tr>
<tr>
<td></td>
<td>cumulative</td>
<td>105</td>
<td>163</td>
<td>160</td>
<td>139</td>
<td>192</td>
<td>249</td>
</tr>
<tr>
<td></td>
<td>constant</td>
<td>95</td>
<td>166</td>
<td>175</td>
<td>173</td>
<td>213</td>
<td>269</td>
</tr>
<tr>
<td>S4</td>
<td>varying</td>
<td>-</td>
<td>-</td>
<td>169</td>
<td>140</td>
<td>207</td>
<td>274</td>
</tr>
<tr>
<td></td>
<td>cumulative</td>
<td>121</td>
<td>197</td>
<td>205</td>
<td>166</td>
<td>238</td>
<td>338</td>
</tr>
<tr>
<td></td>
<td>constant</td>
<td>111</td>
<td>197</td>
<td>220</td>
<td>200</td>
<td>261</td>
<td>352</td>
</tr>
<tr>
<td>S5</td>
<td>varying</td>
<td>-</td>
<td>-</td>
<td>219</td>
<td>169</td>
<td>248</td>
<td>359</td>
</tr>
<tr>
<td></td>
<td>cumulative</td>
<td>140</td>
<td>272</td>
<td>215</td>
<td>297</td>
<td>438</td>
<td></td>
</tr>
<tr>
<td></td>
<td>constant</td>
<td>131</td>
<td>-</td>
<td>272</td>
<td>237</td>
<td>305</td>
<td>438</td>
</tr>
</tbody>
</table>

For cumulative domain semantics the axiom $\forall p, q, w, x. \exists w. R_{px} \land R_{qw} \Rightarrow \exists w. R_{xw}$ is additionally postulated. It states that the individual domains are increasing along relation $R$.

The above approach can be employed in combination with any HOL ATP system (various candidate systems are presented by Sutcliffe and Benzmüller [17]). Here we use LEO-II (http://www.leoprover.org) and Satallax (http://www.ps.uni-saarland.de/~cebrown/satallax). The conversion to thf0-syntax [17] and the provision of the above axioms is realized with the new preprocessor tool FMLtoHOL (1.0) (hence the suffices ‘-M1.0’ on p. 1).

3 Evaluation Summary

The introduced ATP systems were evaluated on all 580 monomodal problems of version 1.1 of the QMLTP library [14]. The QMLTP library is a benchmark library for testing and evaluating ATP systems for FML, similar to the TPTP library for classical logic [18] and the ILTP library for intuitionistic logic [15]. In the experiments the following modal logics were considered: K, D, T, S4, and S5 with constant, cumulative, and varying domain semantics. These modal logics are supported by most of the described ATP systems. All tests were conducted on a 3.4 GHz Xeon system with 4 GB RAM running Linux 2.6.24-24.x86_64. The CPU time limit was set to 600 seconds. All ATP systems and components written in PROLOG use ECLiPSe PROLOG 5.10. LEO-I 1.3.2 was compiled with OCaml 3.12, and uses prover E 1.4. For Satallax a binary of version 2.2 is used. For MSPASS the sources of SPASS 3.0 were compiled using the GNU gcc 4.2.4 compiler.

Table [1] gives an overview of the test results for each prover. It contains the number of proved problems for each considered logic and each domain condition. MleanCoP is the strongest prover for logics D, T, S4 and S5, followed by Satallax. For logic K Satallax performs best. f2p-MSPASS cannot be applied to 299 problems as these problems contain both existential and universal quantifiers. f2p-MSPASS, Satallax and MleanCoP also find counter models for many (invalid) FML formulae. E.g., for T with cumulative domains, these ATP systems found counter models for 89, 90, and 125 problems, respectively. In addition to the 580 monomodal logic problems there are also 20 multimodal logic problems in the QMLTP library. Currently, only Satallax and LEO-II are applicable to them. LEO-II proves 15 of these and Satallax 14. The theorem prover leanTAP 2.3 for first-order classical logic was run on the 580 monomodal problems in the QMLTP library, in which all modal operators have been removed. It (classically) proves 296 problems and refutes one problem.
Acknowledgements. We thank Geoff Sutcliffe and Chad Brown for their valuable input to this work.

References