Liet. matem. rink., T. 43, spec. nr., 438-443
2003 Matematikos ir informatikos institutas

Decision procedure for an extended miniscoped fragment of FTL with equality

Aida PLIUŠKEVIČIENĖ (MII)
e-mail: aida@ktl.mii.lt

1. Introduction

It is well-known that a first-order linear temporal logic FTL is incomplete, in general. But it becomes complete after adding an ω-type rule [2]. We can see the same situation in the case of a first-order linear temporal logic with equality ($FTL_{=}$). This paper is an extension of [4], where a deduction-based decision procedure for a so-called miniscoped fragment of FTL was presented.

The aim of this paper is to present a deduction-based decision procedure for an extended miniscoped fragment of $FTL_{=}$ without function symbols.

2. Sequent calculi considered

Decision procedure presented is justified by means of infinitary calculus $G^{=}_{\omega}$ containing an ω-type rule.

A language is a traditional one for $FTL_{=}$ with temporal operators $\bigcirc$ (Next) and $\Box$ (Always). It is assumed that all the predicate symbols are flexible (i.e., their value changes in time) and constants are rigid (i.e., with time-independent meanings). A term is either a constant or a variable. *An atomic formula* is either an expression of the form $(t_1 = t_2)$ or an expression of the form $P(t_1, \ldots, t_n)$, where P is a predicate symbol, t_i $(1 \leqslant i \leqslant n)$ is a term. A formula is defined in the usual way. As usual, a sequent is an expression of the form $\Gamma \to \Delta$, where Γ, Δ are arbitrary finite multisets of formulas.

DEFINITION 1. Let A be a formula, then A is in *Next-normal form* if each occurrence of the Next operator in A appears only in the subformula of A of the form $\bigcirc^k E$ (here E is an atomic formula, $k \geqslant 0$) and this subformula means a k-time Next atomic formula E.

For the sake of simplicity, we "eliminate" the Next operator and the formula $\bigcirc^k E$ is abbreviated as E^k (i.e., as an atomic formula with the index k). $E^k (k \geqslant 0)$ is called *an elementary formula*, and E^k becomes atomic if $k = 0$.

It is obvious that every formula can be transformed into an equivalent formula in the Next-normal form. For this transformation the following equivalences (valid in $FTL_{=}$, see, e.g., [3]) $\bigcirc(A \odot B) \equiv \bigcirc A \odot \bigcirc B$ $(\odot \in \{\supset, \wedge, \vee\})$ and $\bigcirc \sigma A \equiv \sigma \bigcirc A$ $(\sigma \in$

$\{\neg, \Box, \forall x, \exists x\}$) are used. For an arbitrary formula A, the notation A^k $(k > 0)$ means the Next-normal form of the formula $\bigcirc^k A$. In the sequel there is no difference between formulas of the shape A^k and formulas in Next-normal form and only the latter are considered. A formula not containing either a temporal operator $\Box$ or indices is called *a logical formula*.

A calculus $G^{=}_{\omega}$ is defined by the following postulates.

Axioms: $\Gamma, A \to \Delta, A$; $\Gamma \to \Delta, (t = t)$.

Rules:

1) temporal rules:

$$\frac{A, \Box A^1, \Gamma \to \Delta}{\Box A, \Gamma \to \Delta}\,(\Box \to) \qquad \frac{\Gamma \to \Delta, A; \ldots; \Gamma \to \Delta, A^k; \ldots}{\Gamma \to \Delta, \Box A}\,(\to \Box_\omega) \quad (k \in \omega);$$

2) traditional invertible logical rules for logical operators; for eigen-variables of the rules $(\to \forall)$, $(\exists \to)$ a set of eigen-constants different from other constants is introduced;

3) rules for equality:

$$\frac{(t_1 = t_2), \Gamma^x_{t_2} \to \Delta^x_{t_2}}{(t_1 = t_2), \Gamma^x_{t_1} \to \Delta^x_{t_1}}\,(=_1) \qquad \frac{(t_2 = t_1), \Gamma^x_{t_2} \to \Delta^x_{t_2}}{(t_2 = t_1), \Gamma^x_{t_1} \to \Delta^x_{t_1}}\,(=_2),$$

where the rules $(=_1)$, $(=_2)$ satisfy the following conditions [3]: x is a variable not entering the scope of $\Box$ and indices and it is assumed that the rules $(=_1)$, $(=_2)$ do not create new occurrences of bound variables.

Analogously as in [2], we can prove the following theorem.

Theorem 1. *(a) The calculus $G^{=}_{\omega}$ is sound and complete; (b) the cut rule is admissible in $G^{=}_{\omega}$.*

A calculus $G_{=}$ is obtained from $G^{=}_{\omega}$ by dropping the rule $(\to \Box_\omega)$. A calculus $KG_{=}$ is obtained from $G_{=}$ by dropping the rule $(\Box \to)$.

3. Preliminary to present decision procedure

Using a renaming technique as in [1], we can assume that all formulas in initial sequents considered have an index $n \leqslant 1$. Such renaming allows us to get a more effective decision procedure.

DEFINITION 2. A sequent S is an extended miniscoped sequent (*$EM_{=}$-sequent*) if all, if any, positive (negative) occurrences of $\exists$ ($\forall$, respectively) in the sequent S occur only in a formula of the shape $Q\bar{x}B^k(\bar{x})$, where $Q \in \{\exists, \forall\}$, $\bar{x} = x_1, \ldots, x_n$, $n \geqslant 1$, $k \in \{0, 1\}$, $B(\bar{x})$ is a logical formula not containing positive (negative) occurrences of $\exists$ ($\forall$, respectively) in S. This formula of the shape $Q\bar{x}B^k(\bar{x})$ is called an extended miniscoped formula (*$EM_{=}$-formula*). The $EM_{=}$-formula becomes an atomic $EM_{=}$-formula (*$aEM_{=}$-formula*) if $k = 0$.

Let S be an $EM_{=}$-sequent and $\Gamma = C_1, \ldots, C_i$ ($\Delta = D_1, \ldots, D_j$) be all negative (positive, respectively) occurrences of all $EM_{=}$-formulas in S. Then, a sequent $\Gamma^+ \to \Delta^+$, where $\Gamma^+(\Delta^+)$ is obtained from Γ (Δ, respectively) by dropping indices, if any, from all formulas entering Γ (Δ, respectively), is a *logical image of sequent S denoted by $L(S)$*.

DEFINITION 3. An $EM_{=}$-sequent S is a decidable $EM_{=}$-sequent (*$dEM_{=}$-sequent*), provided that (1) $L(S)$ belongs to a decidable class of a first-order logic with equality (*logical decision condition*); (2) if a formula $\Box A$ occurs negatively in S, then A does not contain positive occurrences of the temporal operator $\Box$ in S (*regularity condition*).

A $dEM_{=}$-sequent S is an *induction-free $dEM_{=}$-sequent*, if S does not contain positive occurrences of $\Box$. Otherwise a $dEM_{=}$-sequent S is a *non-induction-free* one.

Let us introduce some canonical forms of $dEM_{=}$-sequents. An $dEM_{=}$-sequent S is a *primary $dEM_{=}$-sequent*, if $S = \Sigma_1, \Pi_1^1, \Box\Omega_1 \to \Sigma_2, \Pi_2^1, \Box\Omega_2$, where for every i ($i \in \{1, 2\}$) $\Sigma_i = \varnothing$ or consists of $aEM_{=}$-formulas; $\Pi_i^1 = \varnothing$ or consists of $EM_{=}$-formulas; $\Box\Omega_i = \varnothing$ or consists of formulas of the shape $\Box A$. A primary $dEM_{=}$-sequent S is an *indexed primary $dEM_{=}$-sequent* if $\Box\Omega_1, \Box\Omega_2$ consist of formulas of the shape $\Box A^1$.

Now we define rules by which the reduction of an $dEM_{=}$-sequent S to a set of primary and indexed primary $dEM_{=}$-sequents is carried out.

The following rules are called *reduction ones* (all these rules are applied in the bottom-up manner):

1) logical rules of the calculus $G_\omega^{=}$ (except the rules $(\forall \to)$, $(\to \exists)$, and rules for equality);

2) the following temporal rules:

$$\frac{A, \Box A^1, \ \Gamma \to \Delta}{\Box A, \ \Gamma \to \Delta}(\Box^* \to) \quad \frac{\Gamma \to \Delta, A; \ \Gamma \to \Delta, \Box A^1}{\Gamma \to \Delta, \ \Box A}(\to \Box^1),$$

where A in the rules $(\Box^* \to)$, $(\to \Box^1)$ is such that at least one atomic formula is a subformula of A, i.e. A is not a formula of the shape B^1.

Lemma 1. *Let S be a $dEM_{=}$-sequent. Then one can automatically construct a reduction of S to a set $\{S_1, \ldots, S_n\}$, where S_j $(1 \leqslant j \leqslant n)$ is a primary (indexed primary) $dEM_{=}$-sequent; moreover, $G_\omega^{=} \vdash S \Rightarrow G_\omega^{=} \vdash S_j$.*

DEFINITION 4. Let $\Sigma_1, \Pi_1^1, \Box\Omega_1^1 \to \Sigma_2, \Pi_2^1, \Box\Omega_2^1$ be an indexed primary $dEM_{=}$-sequent. Then *separation rule* (SR) is the following rule:

$$\frac{S_1 \text{ or } S_2}{\Sigma_1, \Pi_1^1, \Box\Omega_1^1 \to \Sigma_2, \Pi_2^1, \Box\Omega_2^1} \ (SR)$$

where $S_1 = \Sigma_1 \to \Sigma_2$; $S_2 = \Pi_1, \Box\Omega_1 \to \Pi_2, \Box\Omega_2$.

Lemma 2. *(a) Let S be a conclusion of (SR) and S_i $(i \in \{1,2\})$ means the same as in the rules (SR). Then, if $G^{=}_{\omega} \vdash S$, then either (1) $KG_{=} \vdash S_1$, or (2) $G^{=}_{\omega} \vdash S_2$. (b) The choice of cases* (1) *or* (2) *is deterministic.*

The reduction to a set of primary and indexed primary $dEM_{=}$-sequents along with separation rule (Definition 4) are the main tool to verify saturation (loop) for both induction-free and non-induction-free $dEM_{=}$-sequents and to get decision procedure $EMSat_{=}$ for $dEM_{=}$-sequents.

4. Decision procedure $EMSat_{=}$ for $dEM_{=}$-sequents

Let us introduce some notions which will be used in the decision procedure for arbitrary $dEM_{=}$-sequents.

Let a calculus $G^{+}_{=}$ be obtained from the calculus $G_{=}$ replacing the rule $(\Box \to)$ by the rule $(\Box^* \to)$, and adding the rule (SR).

Lemma 3. *Let S be an induction-free $dEM_{=}$-sequent. Then $G_{=} \vdash S$ if and only if $G^{+}_{=} \vdash S$.*

Two formulas are called *parametrically identical* ones if they are either coincidental, or congruent (i.e., differ only in their bound variables), or differ only by the corresponding occurrences of eigen-variables of the rules $(\to \forall)$, $(\exists \to)$. Two $dEM_{=}$-sequents S and S' are *parametrically identical* (in symbols $S \approx S'$) if S, S' differ only by parametrically identical $EM_{=}$-formulas.

Let us introduce the following structural rule:

$$\frac{\Gamma \to \Delta}{\Pi, \Gamma' \to \Delta', \Theta}\,(W^*), \quad \text{where} \quad \Gamma \to \Delta \approx \Gamma' \to \Delta'.$$

We say that a $dEM_{=}$-sequent S_1 *subsumes* a $dEM_{=}$-sequent S_2 or S_2 is subsumed by S_1 (in symbols $S_1 \succcurlyeq S_2$) if S_2 can be obtained from S_1 using the rule (W^*) (in a special case, $S_1 = S_2$ or $S_1 \approx S_2$).

DEFINITION 5. Let D be a bottom-up deduction consisting of reduction rules and separation rule (SR). A sequent S_j in a node of D is *a saturated sequent* if in the same branch there exists a node with a sequent S_i such that $S_i \succcurlyeq S_j$. A saturated sequent S_j is called a *non-logical axiom*.

Relying on the definition of induction-free $dEM_{=}$-sequent S decision procedure $EMSat_{=}$ for induction-free $dEM_{=}$-sequents follows from the following lemmas.

Lemma 4. *Let S be an induction-free $dEM_{=}$-sequent and D be a bottom-up deduction of S in $G^{+}_{=}$. If in D there exists a branch containing a non-logical axiom then $G^{+}_{=} \nvdash S$.*

Lemma 5. *Let S be an induction-free $dEM_{=}$-sequent. Then an arbitrary deduction of the $dEM_{=}$-sequent S in $G^{+}_{=}$ always terminates.*

A decision procedure $EMSat_{=}$ for a non-induction-free $dEM_{=}$-sequent is based on the verification of *a loop property* (Lemma 6 below). We assume that the notions of the deduction-based decision procedure and the saturation-like calculus are identical. Let $EMSat_{=}$ be a calculus containing reduction rules, separation rule, and logical and non-logical axioms. The verification of a loop property is realized by a saturation-based calculus $EMSat_{=}$.

Our main task is to get a loop property for a primary non-induction-free $dEM_{=}$-sequent.

Lemma 6. *Let S be a primary non-induction-free $dEM_{=}$-sequent. If there exists bottom-up deduction D of S in $EMSat_{=}$ such that each leaf of D is either logical axiom or non-logical one then $EMSat_{=} \vdash S$. Otherwise, $EMSat_{=} \nvdash S$.*

Lemma 7. *Let S be a primary non-induction-free $dEM_{=}$-sequent. Then an arbitrary deduction of the $dEM_{=}$-sequent S in $EMSat_{=}$ always terminates.*

DEFINITION 6. *A procedure $EMSat_{=}$* is applied to a $dEM_{=}$-sequent S. The procedure consists of three points. (1) At first, a redution of S to a set of primary $dEM_{=}$-sequents $S_1, \ldots, S_n$ is constructed (see Lemma 1). (2) If S is an induction-free $dEM_{=}$-sequent, then if, for all i $(1 \leqslant i \leqslant n)$, $G^{+}_{=} \vdash S_i$, then S is derivable in $EMSat_{=}$ $(EMSat_{=} \vdash S)$ (see Lemmas 4, 5). (3) If S is a non-induction-free $dEM_{=}$-sequent, then, if for all $i(1 \leqslant i \leqslant n)$, applying the procedure of loop verification to S_i we get that $EMSat_{=} \vdash S_i$ then S is derivable in $EMSat_{=}$ (see Lemmas 6, 7).

From Lemmas 1, 4, 5, 6, 7 the theorem on decidability of $EMSat_{=}$ follows.

Theorem 2. *Let S be an arbitrary $dEM_{=}$-sequent. Then the procedure $EMSat_{=}$ is decidable for $dEM_{=}$-sequent.*

Analogously as in [4], we can prove the following theorem.

Theorem 3. *Let S be a primary $dEM_{=}$-sequent. Then $EMSat_{=} \vdash S$ if and only if $G^{=}_{\omega} \vdash S$.*

From Theorems 1, 3 the following theorem follows.

Theorem 4. *The calculus $EMSat_{=}$ is sound and complete for the class of $dEM_{=}$-sequents.*

References

[1] M. Fisher, A normal form for temporal logics and its applications in theorem proving and execution, *Journal of Logic and Computation*, **7**(4), 429–456 (1997).
[2] H. Kawai, Sequential calculus for a first-order infinitary temporal logic, *Zeitchr. für Math. Logic and Grundlagen der Math.*, **33**, 423–432 (1987).
[3] Z. Manna, A. Pnueli, Verification of concurrent programs: a temporal proof system, *Foundations of Computer Science*, IV, Amsterdam, Mathematical Centre Tracts, **159**, 163–255 (1983).
[4] R. Pliuškevičius, Deduction-based decision procedure for a clausal miniscoped fragment of FTL, *Lecture Notes in Artificial Intelligence*, **2083**, 107–120 (2001).

Išsprendžiamoji procedūra išplėstam minisferiniam FTL su lygybe fragmentui

A. Pliuškevičienė

Pasiūlyta dedukcija pagrįsta išsprendžiamoji procedūra išplėstam minisferiniam pirmos eilės tiesinio laiko logikos (FTL) su lygybe fragmentui. Pasiūlyta išsprendžiamoji procedūra yra korektiška ir pilna.