

Decision procedure for a fragment of dynamic logic

Aida Pliuškevičienė (MII)

e-mail: aida@ktl.mii.lt

1. Introduction

Dynamic logic [1] has had strong impact on a number of field, including computer science, artificial intelligence and formal theories of knowledge. In this paper first-order dynamic logic, where an atomic program is considered as an arbitrary binary relation and formulas are constructed using first-order logic, is considered. This logic (in short *RDL*) can be used for reasoning about multi-agent system. *RDL* is close to first-order branching-time logic, which is incomplete, in general.

Here we present deduction-based decision procedure for a miniscoped fragment of *RDL*. The main characteristic peculiarity of the proposed procedure is a verification of loop properties (see Lemma 6).

2. Infinitary sequent calculus RD_ω

Decision procedure *MRSat* is justified by means of infinitary calculus RD_ω containing an ω -type rule.

The language of *RDL* consists of the set of predicate symbols, the set of atomic programs, logical symbols and program operators. Programs and formulas are defined inductively, as usual. In the paper $\gamma, \gamma_1, \gamma_2, \dots$ denote atomic programs. A sequent is an expression of the form $\Gamma \rightarrow \Delta$, where Γ, Δ are arbitrary finite multisets of formulas.

DEFINITION 1. A sequent S is *miniscoped sequent* if S satisfies the following miniscoped condition: all negative (positive) occurrences of \forall (\exists , correspondingly) in S occurs only in formulas of the shape QxE , where E is an atomic formula; this formula is called an quasi-atomic formula. Atomic formula is a special case of quasi-atomic formula, if $Qx = \emptyset$

DEFINITION 2. A miniscoped sequent S is *MR-sequent* if S satisfies the following *regularity condition*: let a formula $[\alpha^*]A$ occur negatively in S , then A does not contain positive occurrences of formulas of the shape $[\beta]B$ in S .

A *MR*-sequent S is induction-free *MR*-sequent if S does not contain positive occurrences of formulas $[\beta]A$, where β includes a program of the shape α^* . Otherwise a *MR*-sequent S is non-induction-free one.

The calculus RD_ω is defined by the following postulates.

Axioms:

- 1) $[\alpha^*]A, \Gamma \rightarrow \Delta, [\alpha^*]A$;
- 2) $E(t_1, \dots, t_n), \Gamma \rightarrow \Delta, \exists x_1 \dots x_n E(x_1, \dots, x_n)$;
- 3) $\forall x_1 \dots x_n E(x_1, \dots, x_n), \Gamma \rightarrow \Delta, E(t_1, \dots, t_n)$;
- 4) $\forall x_1 \dots x_n E(t_1(x_1), \dots, t_n(x_n)), \Gamma \rightarrow \Delta, \exists y_1 \dots y_n E(p_1(y_1), \dots, p_n(y_n))$,
where E is a predicate symbol, $\forall i$ ($1 \leq i \leq n$) terms $t_i(x_i)$ and $p_i(y_i)$ are unifiable.

Rules:

Program rules:

$$\frac{\Gamma \rightarrow \Delta, [\alpha] [\beta] A}{\Gamma \rightarrow \Delta, [\alpha; \beta] A} (\rightarrow;)$$

$$\frac{[\alpha] [\beta] A, \Gamma \rightarrow \Delta}{[\alpha; \beta] A, \Gamma \rightarrow \Delta} (; \rightarrow)$$

$$\frac{\Gamma \rightarrow \Delta, [\alpha] A; \Gamma \rightarrow \Delta, [\beta] A}{\Gamma \rightarrow \Delta, [\alpha \cup \beta] A} (\rightarrow \cup)$$

$$\frac{[\alpha] A, [\beta] A, \Gamma \rightarrow \Delta}{[\alpha \cup \beta] A, \Gamma \rightarrow \Delta} (\cup \rightarrow)$$

$$\frac{\{\Gamma \rightarrow \Delta, [\alpha]^k A\}_{k \in \omega}}{\Gamma \rightarrow \Delta, [\alpha^*] A} (\rightarrow [\alpha^*]_\omega)$$

$$\frac{A, [\alpha] [\alpha^*] A, \Gamma \rightarrow \Delta}{[\alpha^*] A, \Gamma \rightarrow \Delta} ([\alpha^*] \rightarrow)$$

$$\frac{A_1, \dots, A_m \rightarrow B_i}{[\gamma] A_1, \dots, [\gamma] A_m, \Gamma \rightarrow \Delta, [\gamma] B_1, \dots, [\gamma] B_n} ([\gamma]),$$

where in $([\gamma])$ $m \geq 0$, $n > 0$, and $1 \leq i \leq n$; in $(\rightarrow [\alpha^*]_\omega)$ $[\alpha]^k A$ means $\overbrace{[\alpha] \dots [\alpha]}^{k\text{-time}} A$.

Logical rules: traditional invertible rules for \supset , \wedge , \vee , \neg , and rules $(\rightarrow \forall)$, $(\exists \rightarrow)$.

Using proof-theoretical methods we can prove that the calculus RD_ω is sound and complete and cut rule is admissible in RD_ω .

The calculus RD is obtained from RD_ω by dropping the rule $(\rightarrow [\alpha^*]_\omega)$.

3. Some auxiliary tools of decision procedure *MRSat*

In this section we present some preparatory steps of the proposed decision procedure *MRSat*.

Let $\{i\}$ denotes a set of rules of some calculus. Then $\{i\}$ -reduction (or briefly, *reduction*) of S to a set of sequents S_1, \dots, S_n (denoted by $R(S)\{i\} \Rightarrow \{S_1, \dots, S_n\}$ or briefly by $R(S)$), is defined to be a tree of sequents with the root S and leaves S_1, \dots, S_n .

and, possibly, axioms of the calculus, such that each sequent in $R(S)$, different from S , is the premise of the rule from $\{i\}$ whose conclusion also belongs to $R(S)$.

DEFINITION 3. A *MR*-sequent S is *reduced* one if $S = \Sigma_1, [\gamma_1]\Pi_1, \dots, [\gamma_n]\Pi_n \rightarrow \Sigma_2, [\gamma]A$, where $\Sigma_i = \emptyset$ ($i \in \{1, 2\}$) or consists of quasi-atomic formulas; $[\gamma_i]\Pi_i = \emptyset$ ($1 \leq i \leq n$) or consists of formulas of the form $[\gamma_i]B_i$ (B_i is an arbitrary formula); A is an arbitrary formula. A *MR*-sequent S is *primary* one, if $S = \Sigma_1, [\alpha_1]\Pi_1, \dots, [\alpha_n]\Pi_n \rightarrow \Sigma_2, [\alpha^*]^0A$, where Σ_1, Σ_2, A means the same as in reduced *MR*-sequent; $\alpha_i \in \{\gamma, \beta^*\}$, where β is an arbitrary program; $[\alpha^*]^0 \in \{\emptyset, [\alpha^*]\}$.

Now we present rules by means of which reductions of a *MR*-sequent to reduced and primary *MR*-sequents are carried out.

Formulas A, A^* are called parametrically identical formulas if either $A = A^*$ or A and A^* are congruent, or A and A^* differ only by corresponding occurrences of eigenvariables of the rules $(\rightarrow \forall)$, $(\exists \rightarrow)$.

The following rules will be called *r-reduction rules* (all these rules, except the contraction rules, will be applied in the bottom-up manner):

- 1) all logical rules of the calculus *RD*;
- 2) the program rules of the calculus *RD*, except the rule $([\gamma])$, and the following program rule:

$$\frac{\Gamma \rightarrow \Delta, A; \Gamma \rightarrow \Delta, [\alpha][\alpha^*]A}{\Gamma \rightarrow \Delta, [\alpha^*]A} (\rightarrow [\alpha][\alpha^*])$$

- 3) the contraction rules, where contraction formulas are quasi-atomic parametrically identical formulas E, E^* .

From the fact that $RD_\omega \vdash [\alpha^*]A \equiv A \wedge [\alpha][\alpha^*]A$ and admissibility of cut rule, we get that the rule $(\rightarrow [\alpha][\alpha^*])$ is admissible and invertible in RD_ω .

The *p-reduction rules* include all *r-reduction rules* and a following separation rule:

$$\frac{S^* = \Pi_1^0, \dots, \Pi_m^0 \rightarrow A_k}{S = \Sigma_1, [\gamma'_1]\Pi_1, \dots, [\gamma'_m]\Pi_m \rightarrow \Sigma_2, [\gamma_1]\Delta_1, \dots, [\gamma_n]\Delta_n} (Sp),$$

where $m \geq 0$, $n > 0$, $\Sigma_i = \emptyset$ ($i \in \{1, 2\}$) or consists of quasi-atomic formulas and the sequent $\Sigma_1 \rightarrow \Sigma_2$ is not an axiom of *RD*; $A_k \in \Delta_i$, because for every i ($1 \leq i \leq n$) $[\gamma_i]\Delta_i$ is a multiset of formulas of the shape $[\gamma_i]A_k$; $\Pi_j^0 = \emptyset$ ($1 \leq j \leq m$) if $\gamma'_j \neq \gamma_i$ ($1 \leq i \leq n$) and $\Pi_j^0 = \Pi_j$ if $\gamma'_j = \gamma_i$.

Lemma 1. Let S be *MR*-sequent. Let S be a conclusion and $S^* = \Pi_1^0, \dots, \Pi_n^0 \rightarrow A_k$ be a premise of the rule (Sp) . Let $\Sigma_1 \rightarrow \Sigma_2$ be not an axiom of RD_ω . If $RD_\omega \vdash S$ then there exists k such that $RD_\omega \vdash S^*$.

Lemma 2. Let S be a *MR*-sequent. Then there exist the following reductions of the sequent S : $R(S)\{i_r\} \Rightarrow \{S_1, \dots, S_n\}$ and $R(S)\{i_p\} \Rightarrow \{S_1^*, \dots, S_m^*\}$, where $\{i_r\}$ is

the set of r -reduction rules and $\{i_p\}$ is the set of p -reduction rules, and S_i ($1 \leq i \leq n$) is a reduced MR -sequent, S_j^* ($1 \leq j \leq m$) is a primary MR -sequent. Moreover, $RD_\omega \vdash S \Rightarrow RD_\omega \vdash S_i$ ($1 \leq i \leq n$) and $RD_\omega \vdash S \Rightarrow RD_\omega \vdash S_j^*$ ($1 \leq j \leq m$).

Proof. The reduction $R(S)\{i_p\} \Rightarrow \{S_1^*, \dots, S_m^*\}$ is carried out by means of the following algorithm.

- 1) Starting from S , let us reduce S (using r -reducing rules) to a set of reduced sequents S_1, \dots, S_n .
- 2) Let us apply bottom-up the rule (Sp) to sequents S_1, \dots, S_n which are not axioms. This rule is applied so many time as it is possible. We get the sequents S_1^*, \dots, S_m^* which are the premises of the last application of the rule (Sp) to the sequents S_1, \dots, S_n , respectively. In common case numbers m and n may be different.
- 3) If $\forall i$ ($1 \leq i \leq m$) S_i^* is a primary MR -sequent then process is finished.
- 4) Let S_i^* is not a primary MR -sequent then $S := S_i^*$ and return to Step 1.

The implication $RD_\omega \vdash S \Rightarrow RD_\omega \vdash S_j^*$ ($1 \leq j \leq m$) follows from the invertibility of r -reduction rules and Lemma 1.

The calculus RD^+ is obtained from the calculus RD replacing the rule $([\gamma])$ by the rule (Sp) which is applied bottom-up. It is evident that only induction-free MR -sequent can be derivable in the calculi RD and RD^+ because these calculi have no rule of the shape $([\rightarrow \alpha^*])$.

Using regularity condition we get that for any induction-free MR -sequent S $RD \vdash S$ iff $RD^+ \vdash S$.

Lemma 3. *The calculus RD^+ is decidable.*

Proof. Using the invertibility of r -reduction rules and Lemma 1.

Let $R(S)\{i_p\} \Rightarrow \{S_1^*, \dots, S_n^*\}$ be a reduction of MR -sequent S to a set of primary MR -sequents. Let us delete from $\{S_1^*, \dots, S_n^*\}$ such primary MR -sequents S_i^* ($1 \leq i \leq n$) which are either axioms of RD^+ or derivable in RD^+ . The obtained reduction is called *the proper reduction* of a MR -sequent S to a set of primary MR -sequents and is denoted by $R^*(S)$.

4. Description of decidable calculus $MRSat$

In this section the decidable calculus $MRSat$ for MR -sequents is described.

We say that the MR -sequents S and S' are parametrically identical (in symbols $S \approx S'$) if the sequents S, S' differ only by parametrically identical formulas.

Let us introduce the following structural rule:

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

We say that a *MR*-sequent S_1 subsumes a *MR*-sequent S_2 or S_2 is subsumed by S_1 (in symbols $S_1 \succ S_2$) if S_2 is a conclusion of an application of the rule (W^*) to S_1 (in a special case $S_1 = S_2$).

The schema of subsumption rule is defined as follows (this rule is applied in the bottom-up manner):

$$\frac{S_1, \dots, S_i^0, \dots, S_{j-1}, S_{j+1}, \dots, S_n}{S_1, \dots, S_i, \dots, S_j, \dots, S_n} (Sm^+),$$

where S_1, \dots, S_n are *MR*-sequents and there exists i ($i \in \{1, \dots, n\}$) such that there exists j ($j \in \{1, \dots, i-1, i+1, \dots, n\}$) and $S_i \succ S_j$. $+ \in \{\emptyset, *\}$. This schema gives us two rules, namely, if $+ = *$ and j is unique then $S_i^0 = \emptyset$, otherwise $S_i^0 = S_i$.

A *subsumption-tree* (denoted by (ST^+)) of *MR*-sequents S_1, \dots, S_n is defined by the following bottom-up deduction:

$$\left. \begin{array}{l} \frac{S_1^*, \dots, S_k^*}{\dots \dots} (Sm^+) \\ \frac{\dots \dots}{S_1, \dots, S_n} (Sm^+) \end{array} \right\} (ST^+),$$

where the set of *MR*-sequents $M = \{S_1^*, \dots, S_k^*\}$ is such that it is impossible to apply (Sm^+) to the set M . The sequents from (ST^+) which subsumes some sequents from (ST^+) will be called *active part* of (ST^+) , and the sequents of (ST^+) which are subsumed will be called *passive part* of (ST^+) .

Let $R^*(S)$ be the proper reduction of *MR*-sequent S to a set of primary sequents S_1^*, \dots, S_m^* . Then the *resolvent-tree* of a *MR*-sequent S is defined by the following bottom-up deduction (denoted by $ReT(S)$):

$$\left. \begin{array}{l} \frac{S_1 \dots S_n}{S_1^* \quad \vdots \quad S_m^*} (ST) \\ \left. \begin{array}{l} \backslash \quad \vdots \quad / \\ \backslash \quad \vdots \quad / \\ S \end{array} \right\} R^*(S) \end{array} \right\} ReT(S).$$

The set $\{S_1, \dots, S_n\}$ of primary sequents is *resolvent* of *MR*-sequent S and is denoted by $Re(S)$. If the set $\{S_1^*, \dots, S_m^*\}$ contains induction-free *MR*-sequent, then the construction of $ReT(S)$ is unsuccessful (in symbols $ReT(S) = \perp$). If the set $\{S_1^*, \dots, S_m^*\}$ is empty then $Re(S) = \emptyset$.

From Lemmas 2 and 3 we get

Lemma 4. *Let S be a *MR*-sequent, then the problem of construction of $ReT(S)$ is decidable.*

To define the main deductive procedure of the proposed decision saturation-based procedure *MRSat* let us introduce some auxiliary notions.

DEFINITION 4. A set of *R*-subformulas of a formula *A* from *MR*-sequent *S* (denoted by $RSub(A)$) is defined inductively.

1. $RSub(E) = \emptyset$, where *E* is a quasi-atomic formula.
2. $RSub([\gamma]E) = E$, where *E* is an quasi-atomic formula.
3. $RSub([\gamma]A) = \{[\gamma]A\} \cup RSub(A)$.
4. $RSub(\neg A) = RSub(A)$.
5. $RSub(A \odot B) = RSub(A) \cup RSub(B)$, where \odot is a logical operator.
6. $RSub(Qx B(x)) = RSub(B(c_0))$, where *Q* is \forall (\exists) and occurs positively (negatively) in *S* and c_0 is a new constant.
7. $RSub([\alpha^*]A) = \{[\alpha^*]A\} \cup RSub(A)$.
8. Let *E* and E_1 are parametrically identical quasi-atomic formulas, and $E \in RSub(A)$. Then $E_1 \in RSub(A)$.

A set of *R*-subformulas of a primary *MR*-sequent $S = A_1, \dots, A_n \rightarrow B_1, \dots, B_m$ is denoted by $RSub(S)$ and defined as follows: $RSub(S) = \bigcup_{i=1}^n RSub(A_i) \cup \bigcup_{i=1}^m RSub(B_i)$.

$R^*Sub(S)$ means the set obtained from $RSub(S)$ by merging the formulas that are parametrically identical. The set $RSub(S)$ is parametrically finite if $R^*Sub(S)$ is finite.

From Definition 4 we get

Lemma 5. Let *S* be a *MR*-sequent, then the set $R^*Sub(S)$ is finite.

Now we define the main deductive tool of the proposed decision procedure *MRSat*, which will be applied to a primary *MR*-sequent. Let us define *k*-th resolvent-tree $Re^k T(S)$ and *k*-th resolvent $Re^k(S)$ of a primary *MR*-sequent *S*.

DEFINITION 5. Let *S* be a primary *MR*-sequent. If *S* is an axiom then $Re^0(S) = \emptyset$, otherwise $Re^0(S) = Re^0 T(S) = S$. Let $Re^k(S) = \{S_1, \dots, S_n\}$, then $Re^{k+1}(S)$ and $Re^{k+1} T(S)$ are defined by the following bottom-up deduction:

$$\frac{\frac{\frac{Re(S_1)}{S_1} ReT(S_1) \dots \frac{Re(S_n)}{S_n} ReT(S_n)}{\underbrace{\hspace{10em}}_{Re^k(S)}} \quad \frac{Re_p^{k+1}(S)}{(ST)} \quad \left(\bigcup_{i=0}^k Re^i(S) \right)^*}{Re^{k+1}(S)} (ST^*)$$

The bottom-up application of (ST) reduces the set $\bigcup_{i=1}^n Re(S_i)$ to a preliminary resolvent $Re_p^{k+1}(S)$ of primary *MR*-sequents. In the bottom-up application of (ST^*) the

sequents from $(\bigcup_{i=0}^k Re^i(S))^*$ are active part of the application of (ST^*) and the sequents from $Re_p^{k+1}(S)$ are passive one. $(\bigcup_{i=0}^k Re^i(S))^*$ is obtained from $\bigcup_{i=0}^k Re^i(S)$ deleting all sequents which are not used as active part of (ST^*) . The bottom-up application of (ST^*) reduces the set $Re_p^{k+1}(S) \cup (\bigcup_{i=0}^k Re^i(S))^*$ to the set $Re^{k+1}(S)$ which will be called $(k+1)$ -th resolvent of a primary MR -sequent S . If $\exists i (1 \leq i \leq n)$ such that $ReT(S_i) = \perp$ then $Re^{k+1}(S) = \perp$ and $Re^{k+1}T(S) = \perp$, i.e., the construction of $Re^{k+1}T(S)$ is not successful. The set $Re^{k+1}(S)$ is empty in two following cases: either $\forall i (1 \leq i \leq n) Re(S_i) = \emptyset$, or the bottom-up application of (ST^*) in $Re^{k+1}T(S)$ yields the empty set.

Notation $Re^kT(S) \neq \perp (k \in \omega)$ means that the construction of $Re^kT(S)$ is successful for all $k \in \omega$.

Now we establish the main property of the procedure of construction of $Re^kT(S)$.

From Lemma 5 and Definition 6 we get

Lemma 6. *Let S be a primary MR -sequent and $Re^kT(S) \neq \perp (k \in \omega)$. Then there exists finite natural number p such $Re^p(S) = \emptyset$.*

From Lemmas 3, 5, 6 we get

Lemma 7. *The relation $Re^p(S) = \emptyset$ is decidable.*

Let S be a induction-free MR -sequent, then the calculus $MRSat$ coincides with the calculus RD^+ . An induction-free MR -sequent is derivable in $MRSat$ (in symbols $MRSat \vdash S$) if $RD^+ \vdash S$, otherwise $MRSat \not\vdash S$. Let S be a non-induction-free MR -sequent, then $MRSat$ is described by two procedures:

(1) procedure of reduction of S to a set of primary sequents $Re(S) = \{S_1, \dots, S_n\}$,

(2) the procedure of construction of k -th resolvent $Re^k(S_i)$, where $(1 \leq i \leq n)$.

We say that $MRSat \vdash S$ if either $Re(S) = \emptyset$ or $Re(S) = \{S_1, \dots, S_n\}$, and $\forall i (1 \leq i \leq n) Re^k(S_i) = \emptyset$. Otherwise $MRSat \not\vdash S$.

From Lemmas 3, 6 we get

Lemma 8. *The calculus $MRSat$ is decidable for any MR -sequent.*

Theorem 1. *Let S be a MR -sequent, then $RD_\omega \vdash S \iff MRSat \vdash S$. Thus the calculus $MRSat$ is sound and complete.*

References

Išsprendžiamoji procedūra dinaminės logikos fragmentui

A. Pliuškevičienė

Pasiūlyta dedukcija pagrįsta išsprendžiamoji procedūra miniskopizuotam pirmos eilės dinaminės logikos fragmentui. Pasiūlyta išsprendžiamoji procedūra yra korektiška ir pilna.