*Liet. mat. rink. LMD darbai*, **48/49**, 2008, 283–287

# Loop-free verification of termination of derivation for a fragment of dynamic logic

Regimantas PLIUŠKEVIČIUS (MII)
e-mail: regis@ktl.mii.lt

**Abstract.** A fragment of a deterministic propositional dynamic logic ($DPDL$, in short) is considered The language of considered fragment contains propositional symbols, action constants, action operator (repetition) and logical symbols. For safety fragment of considered $DPDL$ a loop-check-free sequent calculus with invertible rules is presented.

*Keywords:* propositional dynamic logic, sequent calculus, loop-check, invertible rule.

## 1. Introduction

In the paper deterministic propositional dynamic logic ($DPDL$, in short) is considered. In $DPDL$ atomic program (or action constant) in each state specifies at most one successor state. $DPDL$ is a generalization of propositional linear temporal logic ($PLTL$, in short). It is well known (see, e.g., [3], [4]) that with the aim to get termination of derivations in sequent (or tableaux) calculus for $DPDL$ "good loops" (related with induction-like rules) and "bad loops" (related with induction-free parts of derivations) are used. For $PLTL$ verification of "good loops" was proposed in [5], [1] and verification of "bad loops" for induction-free non-classical logics was proposed in [2].

The aim of this paper is to construct loop-check-free sequent calculus for a fragment of $DPDL$. Instead of both types of loop checking special "final" sequents are used. These "final" sequents allow us to verify a termination of derivations without loop checking.

## 2. Initial sequent calculus for $DPDL$

The *language* of considered $DPDL$ contains: a set of propositional symbols $P, P_1, \ldots$, $Q, Q_1, \ldots$ (called atomic formulas); a set of action constants $\gamma, \gamma_1, \gamma_2, \ldots$ (called atomic programs); action operator $*$ (repetition); logical operators: $\supset$, $\wedge$, $\vee$, $\neg$.

We do not consider action constructions ; (composition), $\cup$ (non-deterministic choice), and ? (test) because we concentrate on the induction-like operator $*$.

Programs (*actions*) and *formulas* of $DPDL$ are defined inductively. For example, $\gamma, \gamma^*, (\gamma^*)^*$ are actions. Logical formulas are defined in the usual way. Let $A$ is a formula and $\alpha$ is an action, then $[\alpha]A$ is a formula, $[\alpha]$ is an *action modality*. The formula $[\alpha]A$ means: every possible execution of the action $\alpha$ leads to a situation in which $A$ is true. Therefore the formula $[\alpha]A$ means the same as the formula $True \supset \{\alpha\}A$ in Hoare-type logic.

We consider sequents, i.e., formal expressions $A_1, \ldots, A_k \to B_1, \ldots, B_m$, where $A_1, \ldots, A_k$ $(B_1, \ldots, B_m)$ is a multiset of formulas. A subformula (or some symbol) occurs *positively* in some formula $B$ if it appears within the scope of an even number of the negation sign, once all the occurrences of $A \supset C$ have been replaced by $\neg A \vee C$; otherwise the subformula (symbol) occurs *negatively* in $B$. For a sequent $S = A_1, \ldots, A_k \to B_1, \ldots, B_m$ positive and negative occurrences are determined just like for the formula $\bigwedge_{i=1}^{k} A_i \supset \bigvee_{j=1}^{m} B_j$.

Let $G$ be some sequent calculus and $(i)$ be any inference rule of $G$. A rule $(i)$ is applied to get the conclusion of $(i)$ from the premises of $(i)$. If rule $(i)$ is backward applied, i.e., to get premises of $(i)$ from the conclusion of $(i)$ we have a "backward application of $(i)$" instead of "application of $(i)$". As usual, proof search in sequent calculi is implemented as a backward derivation, i.e., applying the rules backwards. Let $S$ be a sequent, then the notation $G \vdash^V S$ means that $S$ is derivable in $G$ and $V$ is a derivation of $S$ in $G$, i.e., a tree each branch of which ends with an axiom. Let $G \vdash^V S$, and $S$ is the conclusion of a rule $(i)$, $S_j$ is any premise of $(i)$. Then the rule $(i)$ is *invertible* in $G$, if for all $j$ there exists such a derivation $V_j$ of $S_j$ in $G$ that $G \vdash^{V_j} S_j$. Let $G + (j)$ means a calculus obtained from $G$ by adding a rule $(j)$. A rule $(j)$ is *admissible* rule in $G$, if from $G + (j) \vdash^V S$ follows that there exists $V^*$ such that $G \vdash^{V^*} S$.

An initial sequent calculus $GDPDL$ for considered $DPDL$ is defined by the following postulates:

**Axiom:** $\Gamma, A \to \Delta, A$.

The formula $A$ is called the *main formula* of the axiom.

**Logical rules:**

Traditional rules for logical connectives $\supset$, $\wedge$, $\vee$, $\neg$.

**Action rules:**

$$\frac{\Gamma_1 \to \Gamma_2}{\Pi, [\gamma]\Gamma_1 \to \Delta, [\gamma]\Gamma_2}\,([\gamma]),$$

where $[\gamma]\Gamma_i$ $(i \in \{1, 2\})$ is empty or consists of formulas of the shape $[\gamma]A$.

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

where the formula $I$ (called an invariant formula) is constructed using formulas from the conclusion of the rule $(\to *)$. The rule $(\to *)$ corresponds to the induction-like axiom $A \wedge [\alpha^*](A \supset [\alpha]A) \supset [\alpha^*]A$.

From [3], [4] it follows that the calculus $GDPDL$ is sound and complete.

## 3. Elimination of loop-check for fragment of $DPDL$

In this section a *safety* fragment of $DPDL$ is described and loop-check-free sequent calculus for this fragment is constructed.

A positive occurrence of action modality $[\mathcal{Q}]$ $(\mathcal{Q} \in \{\alpha^*, \gamma\})$ in a sequent $S$ is a *special* one if it occurs within the scope of a negative occurrence of operator $[\alpha^*]$

in $S$. A sequent $S$ is a *safety* one if it does not contain special occurrences of action modality $[\mathcal{Q}]$.

For example, the sequent $[\gamma^*][\gamma]P \to [\gamma^*][\gamma^*]P$ is safety but the sequent $[\gamma^*]\neg[\gamma]P \to [\gamma^*][\gamma^*]P$ is not safety.

To eliminate mentioned in the introduction two type of loop-check let us introduce a *marked action modality* $[\mathcal{Q}]^+$ (along with ordinary action modality $[\mathcal{Q}]$) and *marked atomic formulas* of the shape $P^+$ (along with non-marked ones). The marked action modality $[\mathcal{Q}]^+$ and marked atomic formulas are used to define special final sequents which allow us to exclude loop checking.

The marking is defined inductively as follows:

$(P^\sigma)^+ = P^+$ where $\sigma \in \{\varnothing, +\}$ and $P$ is an atomic formula; $(M \odot N)^+ = M^+ \odot N^+$ where $\odot \in \{\wedge, \vee, \supset\}$; $(\delta M)^+ = \delta M^+$ where $\delta \in \{\neg, [\alpha^*]\}$; $([\gamma]^\sigma M)^+ = [\gamma]^+ M^+$ where $\sigma \in \{\varnothing, +\}$.

The sequent $S$ is *induction-like final* (*$i$-final*, in short) sequent if $S$ has a shape $\Sigma_1^+, [\gamma_1]^+\Gamma_1, \ldots, [\gamma_n]^+\Gamma_n, [\alpha_1^*]^+\Pi_1, \ldots, [\alpha_m^*]^+\Pi_m \to \Sigma_2^+, [\beta_1^*]^+\Delta_1, \ldots, [\beta_l^*]^+\Delta_l$, where $\Sigma_i^+$ ($i \in \{1, 2\}$) is empty or consists of marked atomic formulas and $\Sigma_1^+ \cap \Sigma_2^+ = \varnothing$; $n \geqslant 0,\ m \geqslant 0,\ l > 0$. The $i$-final sequents replace the induction type loops.

The sequent of the shape $\Gamma \xrightarrow{r} \Delta$ (called *regular*) are used to distinguish between "induction-type" parts of derivation (i.e., the parts containing applications of the rule for positive occurrence of action modality $[\alpha^*]$) and "non-induction-type" parts of derivation (i.e., the parts not containing applications of the mentioned rule).

The sequent $S$ is *regular final* (*$r$-final*, in short) sequent if $S$ has a shape $\Sigma_1^\sigma, [\gamma_1]^+\Gamma_1, \ldots, [\gamma_n]^+\Gamma_n, [\gamma_{n+1}][\alpha_1^*]^+\Pi_1, \ldots, [\gamma_{n+m}][\alpha_m^*]^+\Pi_m \xrightarrow{r} \Sigma_2^\sigma$, where $\sigma \in \{\varnothing, +\}$, $\Sigma_1^\sigma \cap \Sigma_2^\sigma = \varnothing$; $n \geqslant 0,\ m \geqslant 0$.

A loop-check-free calculus $G_1DPDL$ is obtained from the calculus $GDPDL$ by the following transformations:

- The rule $(* \to)$ is replaced by the following one:

$$\frac{A^+, [\alpha][\alpha^*]^+A, \Gamma \xrightarrow{\lambda} \Delta}{[\alpha^*]A, \Gamma \xrightarrow{\lambda} \Delta}\ (*^+ \to),$$

where $\lambda \in \{\varnothing, r\}$; in the conclusion of the rule the outmost action modality $[\alpha^*]$ in the formula $[\alpha^*]A$ is not marked.

- The rule $(\to *)$ is replaced by the following one:

$$\frac{\Gamma \xrightarrow{r} \Delta, A^+;\ \Gamma \to \Delta, [\alpha][\alpha^*]^+A}{\Gamma \xrightarrow{\lambda} \Delta, [\alpha^*]A}\ (\to *^+),$$

where $\lambda \in \{\varnothing, r\}$; in the conclusion of the rule the outmost action modality $[\alpha^*]$ in the formula $[\alpha^*]A$ is not marked. In spite of the conclusion of the rule is regular or not, the left premise always is a regular sequent, while the right premise is not a regular sequent. This rule is exactly one that *introduces the regular sequents*.

• The rule $([\gamma])$ is replaced by the following two rules (for simplicity these rules are formulated with one action constant):

$$\frac{\Pi_1, [\alpha^*]\Gamma \stackrel{\lambda}{\to} \Pi_2, [\beta^*]\Delta}{\Sigma_1^{\sigma_1}, [\gamma]^{\mu}\Pi_1, [\gamma][\alpha^*]^+\Gamma \stackrel{\lambda}{\to} \Sigma_2^{\sigma_2}, [\gamma]\Pi_2, [\gamma][\beta^*]^+\Delta}\ ([\gamma]^-),$$

where $\lambda \in \{\varnothing, r\}$ and the conclusion of the rule is not $r$-final sequent; $\Sigma_1^{\sigma_1} \cap \Sigma_2^{\sigma_2}$ is empty, $\sigma_i \in \{\varnothing, +\}$, $\mu \in \{\varnothing, +\}$; $[\gamma]^{\mu}\Pi_1 \cup [\gamma]\Pi_2$ is not empty, and if $[\gamma]\Pi_2$ is empty then $[\gamma]^{\mu}\Pi_1$ contains at least one formula different from $[\gamma]^+A$ where $A \neq [\alpha^*]B$. In special case, the conclusion of the rule does not contain marks.

$$\frac{\Pi, [\alpha^*]^+\Gamma \to [\beta^*]\Delta}{\Sigma_1, [\gamma]^+\Pi, [\gamma][\alpha^*]^+\Gamma \to \Sigma_2, [\gamma][\beta^*]^+\Delta}\ ([\gamma]^+),$$

where $\Sigma_1 \cap \Sigma_2$ is empty.

• The sequent of the shape $\Gamma, A^{\tau} \stackrel{\lambda}{\to} \Delta, A^{\sigma}$, where $\lambda \in \{\varnothing, r\}$, $\tau \in \{\varnothing, *\}$, $\sigma \in \{\varnothing, *\}$, is a *logical axiom.*

• Any $i$-final sequent is *non-logical axiom.*

It is obvious that all rules of $G_1DPDL$ are invertible.

A derivation $V$ of a sequent $S$ in the calculus $G_1PLTL$ is a *successful* one, if *each* branch of $V$ ends with a logical axiom or $i$-final sequent. In this case a sequent $S$ is derivable in $G_1DPDL$. A derivation $V$ of $S$ in the calculus $G_1DPDL$ is an *unsuccessful* one if $V$ contains a branch ending with a $r$-final sequent. In this case a sequent $S$ is non-derivable.

An end-sequent of a derivation in calculus $G_1DPDL$ does not contain occurrences of marked modalities or marked atomic formulas. On the other hand, since $r$-final sequent is used as stopping device for non-derivability in $G_1DPDL$, it is assumed that end-sequent of a derivation in calculus $G_1DPDL$ is regular sequent $S_r$ of the shape $\Gamma \stackrel{r}{\to} \Delta$.

*Example 1.* (a) Let $S$ be a sequent $Q, P, [\gamma^*]A \to [\gamma^*]P$, where $A = (P \supset [\gamma]P)$. Let us construct a derivation of $S$ in $G_1DPDL$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{S^* = P^+, [\gamma^*]^+A \to [\gamma^*]^+P}{Q, [\gamma][\gamma^*]^+A, P \stackrel{r}{\to} [\gamma][\gamma^*]^+P, P^+;\ \ Q, P, [\gamma]^+P^+, [\gamma][\gamma^*]^+A \to [\gamma][\gamma^*]^+P}\ (\supset\to)}{Q, P, (P \supset [\gamma]P)^+, [\gamma][\gamma^*]^+A \to [\gamma][\gamma^*]^+P}\ (*^+\to)}{Q, P, [\gamma^*](P \supset [\gamma]P) \stackrel{r}{\to} P;\ \ Q, P, [\gamma^*](P \supset [\gamma]P) \to [\gamma][\gamma^*]^+P}\ (\to *^+)}{S = Q, P, [\gamma^*](P \supset [\gamma]P) \stackrel{r}{\to} [\gamma^*]P}\ ([\gamma]^+)$$

Since $S^*$ is $i$-final sequent $G_1DPDL \vdash S_r$.

(b) Let $S = [\gamma^*][\gamma]P \to [\gamma]Q$. Let us construct a derivation of $S$ in $G_1DPDL$:

$$\dfrac{\dfrac{\dfrac{S^* = P^+, [\gamma]^+P^+, [\gamma][\gamma^*]^+[\gamma]P \overset{r}{\to} Q}{P^+, [\gamma^*]^+[\gamma]P \overset{r}{\to} Q}(*^+ \to)}{[\gamma]^+P^+, [\gamma][\gamma^*]^+[\gamma]P \overset{r}{\to} [\gamma]Q}([\gamma]^-)}{S_r = [\gamma^*][\gamma]P \overset{r}{\to} [\gamma]Q}(*^+ \to)$$

Since $S^*$ is $r$-final sequent $G_1DPDL \nvdash S_r$.

THEOREM 1. *The calculus $G_1DPDL$ is loop-check-free, and $GPLTL \vdash S$ if and only if $G_1PLTL \vdash S_r$ where $S$ is a safety sequent.*

## References


1. G.D. Gough, *Decision Procedures for Temporal Logic*, Master's thesis, Department of Computer Science, Manchester University, Oxford Rd., Manchester, M139PL, UK, (1984).
2. M. Fitting, *Proof Methods for Modal and Intuitionistic Logics*, *Synthese Library*, **169**, D. Reidel, Dordrecht, Holland (1983).
3. V.R. Pratt, A practical decision method for propositional dynamic logic, in: *10th ACM Symposium on the Theory of Computation* (1977), pp. 326–337. A revised version appears as: A near optimal method for reasoning about action, *J. Comput. Systems Sci.*, **20**, 231–254 (1980).
4. M.K. Valiev, On axiomatization of deterministic propositional dynamic logic, in: *Proc. of Symposium on the Mathematical Foundations of Computer Science* (1979), pp. 482–491.
5. P. Wolper, The tableaux method for temporal logic: an overview, *Logique et Analyse*, **28**, 119–136 (1985).



REZIUMĖ

***R. Pliuškevičius. Beciklis įrodymų baigtinumo tikrinimas dinaminės logikos fragmentui***

Straipsnyje yra nagrinėjama determinuota propozicinė dinaminė logika. Sukonstruotas beciklis sekvencinis skaičiavimas šios logikos fragmentui. Ciklų tikrinimas yra pakeičiamas tam tikro pavidalo sekvencijomis.



*Raktiniai žodžiai*: propozicinė dinaminė logika, sekvencinis skaičiavimas, ciklų tikrinimas, apverčiama taisyklė.