INFORMATICA, 2008, Vol. 19, No. 4, 597–616
© 2008 *Institute of Mathematics and Informatics, Vilnius*

Termination of Derivations in a Fragment of Transitive Distributed Knowledge Logic

Regimantas PLIUŠKEVIČIUS, Aida PLIUŠKEVIČIENĖ
Institute of Mathematics and Informatics
Akademijos 4, LT-08663 Vilnius, Lithuania
e-mail: {regis, aida}@ktl.mii.lt

Received: February 2008; accepted: June 2008

Abstract. A transitive distributed knowledge logic is considered. The considered logic $S4_nD$ is obtained from multi-modal logic $S4_n$ by adding transitive distributed knowledge operator. For a fragment of this logic loop-check-free sequent calculus is proposed. The considered fragment is such that it can be applied for specification and verification of safety properties of knowledge-based distributed systems. By relying on the constructed loop-check-free sequent calculus a PSPACE procedure to determine a termination of backward derivation in considered fragment of the logic $S4_nD$ is presented.

Keywords: logic of knowledge, distributed knowledge, safety and liveness properties of distributed systems, deduction-based decision procedure, sequent calculus, loop-check, backtracking, PSPACE-complexity.

1. Introduction

Knowledge-based logics have been widely applied in CS, AI, social sciences and economics as they provide a simple and intuitive language that has proven effective at capturing important concepts treated in such fields as knowledge representation, knowledge-based computer systems, software engineering, especially in distributed systems, and capturing these concepts in a computationally tractable manner.

To consider properties of distributed systems logics of knowledge with distributed knowledge operator were introduced in (Fagin and Vardi, 1986; Fagin *et al.*, 1992; Halpern and Moses, 1992; Fagin *et al.*, 1995). The completeness of Hilbert-style calculi for these logics was proved in (Fagin *et al.*, 1992; Halpern and Moses, 1992; Fagin *et al.*, 1995; Meyer and van der Hoek, 1995). The decidability (based on finite model property) of the logics with distributed knowledge was proved in (Fagin *et al.*, 1995). Distributed knowledge, sometimes also called "implicit knowledge", cannot be defined in terms of "everybody knows" or common knowledge (Fagin *et al.*, 1995). Distributed knowledge is the knowledge that is implicitly present in a group of agents, and which might become explicit if the agents were able to communicate. Intuitively, distributed knowledge is the knowledge that can be obtained when the agents (from some agent group) pool their knowledge. If we have only one agent the distributed knowledge reduces to knowledge. Specification of distributed knowledge logics is a good preparation to study much more complicated common knowledge axiomatics and semantics of which is defined with a help of some induction-like axiom (see, e.g., (Fagin *et al.*, 1995; Meyer and van der Hoek, 1995)).

One of the main tasks in the field of knowledge-based logics is to find *decision procedures* allowing us to tell in an automatic way whether the given knowledge-based specifications are provable (or true) in some logical formalism. Along with the model based approach (e.g., (Clarke *et al.*, 2000)), a deductive approach (based on logical calculi) is widely used. In a deductive approach various formal calculi are used. For non-classical logics tableaux (see, e.g., (Fitting, 1996)) and Gentzen-style (sequent) (see, e.g., (Gallier, 1986)) calculi are most often employed because these calculi are more suitable to construct derivations in rather convenient way. Deduction-based decision procedures will not only tell us whether a given specification is provable (true) or not, but also give the proof of the specification whenever it is provable.

A proof that suitable logical calculus (e.g., sequent or tableaux calculus) allows us to get a decision procedure is crucial but it is not enough. Check of *termination* of a decision procedure is very important problem and though termination of a decision procedure is a strict requirement, it may be hard to establish. Termination of various processes is a fundamental topic in CS. Check of termination of a decision procedure often require to keep information on previous parts of a derivation.

Traditional techniques used to ensure termination of a decision procedure in non-classical (e.g., knowledge-based) sequent (and tableau) calculi is based on *loop-check* (Fitting, 1983; Fitting, 1993; Goré, 1999). Namely, before applying any rule it is checked if this rule was already applied to “essentially the same” sequent; if this is the case we block the application of the rule. Naive methods which store all previously seen nodes are typically not effective. Therefore unrestricted loop-check is often considered as useless (see,e.g., (Demri, 1995)). In (Heuerding *et al.*, 1996), efficient loop-check for modal logic $S4$, tense logic K_t, and a fragment of intuitionistic logic was presented using sequents extended by the notion of a history. For modal logic KT loop-check-free sequent calculus is presented in (Heuerding *et al.*, 1996) using sequents with two halves. In (Dyckhoff, 1992; Hudelmaier, 1992) a contraction-free calculus for propositional intuitionistic logic was proposed. A contraction-free calculus entirely excludes loop-check in derivations. In (Hudelmaier, 1996), a contraction-free calculus for $S4$ was constructed, however only for sequents in Mints normal form. Alternative approach (Fitting, 1993; Cerrito and Cialdea Mayer, 1997) is to translate a considered modal logic into a more simple modal logic. Interesting approach is proposed in (Massacci, 2000) allowing us to decrease a complexity of loop-check for various modal logics. Decision procedures allowing us to specialize the structure of derivations are proposed in (Pliuškevičius and Pliuškevičienė, 2004) (for temporal logic of belief and actions) and in (Pliuškevičius and Pliuškevičienė, 2006) (for a fragment of mutual belief logic with quantified agent variables).

Considering deductive decision procedures *backtracking* is one more problem. This problem is related with the presence (in general case) of non-invertible rules in a sequent (or tableaux) calculus. Invertibility property is very significant because it allows to preserve derivability when applying the rules backwards to construct derivations in an *automatic* way. Traditional invertibility of all rules of a calculus allows us to construct derivations without backtracking. As usual, sequent (or tableaux) calculi for non-classical logics contain non-invertible rules. There are several techniques to get invertibility or to restrict backtracking in sequent calculi for non-classical logics. One method is to use indexation technique. Using this technique invertible sequent calculi for modal logic $S5$ (Kanger, 1957) and for intuitionistic logic (Maslov, 1967) were constructed. Another method is to use specialization of rules which allow us to eliminate or restrict backtracking. In (Pliuškevičius and Pliuškevičienė, 2006) a method is proposed to replace non-invertible rules by existentially invertible ones. In contrast to usual invertibility, existential invertibility requires a restricted backtracking.

In (Fagin and Vardi, 1986; Fagin *et al.*, 1992; Halpern and Moses, 1992; Fagin *et al.*, 1995; Meyer and van der Hoek, 1995) distributed knowledge logics based on various multi-modal logics were considered. But only *transitive* distributed knowledge logics, i.e., containing transitive axioms, are really important for applications of these logics in CS, AI and other fields. The transitive axioms in distributed knowledge logics allow us to apply these logics for specification and verification of distributed systems.

In this paper a transitive distributed knowledge logic $S4_nD$ is considered. The logic $S4_nD$ is obtained from multi-modal logic $S4_n$ by adding distributed knowledge operator. An initial Gentzen-style calculus for $S4_nD$ contains two modal reflexivity rules which correspond to reflexivity axioms, two modal transitivity rules which correspond to transitivity axioms, and a modal interaction rule which corresponds to axiom of interaction between knowledge and distributed knowledge. The premise of reflexivity and transitivity rules preserve some modal formulas from the conclusion of the rules. Unlike the other rules, the transitivity and interaction rules are not invertible. For these reasons backward proof search requires a loop-check and backtracking, in general.

The aim of this paper is to present a procedure without loop-check for determination of a termination of backward derivation in a fragment of distributed knowledge logic $S4_nD$. The considered fragment is such that it can be applied for specification and verification of *safety properties* of knowledge-based distributed systems (see, e.g., (Halpern, 1987; Fagin *et al.*, 1997; Huth and Ryan, 2000; Yoshioka *et al.*, 2001)) and will be called a safety fragment. The procedure proposed in this paper is carried out using a sequent calculus. This calculus does not require sequents in a certain normal form and does not use sequents with two halves. With a view to avoid loop-check, applications of reflexivity and transitivity rules are restricted using marked knowledge and distributed knowledge operators. An existential invertibility (see, e.g., (Pliuškevičius and Pliuškevičienė, 2006)) of the transitivity and interaction rules allows us to restrict backtracking. It is demonstrated that presented technique *does not allow* us to exclude loop-check in *non-restricted* distributed knowledge logic $S4_nD$ which is suitable for specification and verification of *liveness properties* of distributed systems (see, e.g., (Halpern, 1987; Fagin *et al.*, 1997; Huth and Ryan, 2000; Yoshioka *et al.*, 2001)).

The paper is organized as follows. In Section 2, Hilbert-style and Gentzen-style calculi for the logic $S4_nD$ are described. In Section 3, specialization of reflexivity rules is presented. In Section 4, an existential invertibility of the transitivity and interaction rules is established. In Section 5, a PSPACE procedure for determination of termination of backward proof search in considered safety fragment of the logic $S4_nD$ is presented. In Section 6, conclusions and further investigations are briefly discussed. In Appendix some lemmas from Sections 2 and 3 are proved.

2. Hilbert-Style and Gentzen-Style Calculi for the Logic $S4_nD$

The logic $S4_nD$ is obtained from the multi-modal logic $S4_n$ by adding distributed knowledge operator $\mathbf{D}$ (see, e.g., (Fagin and Vardi, 1986; Fagin *et al.*, 1992; Halpern and Moses, 1992; Fagin *et al.*, 1995; Meyer and van der Hoek, 1995)).

A *language* of this logic contains: a set of propositional symbols $P, P_1, P_2, \ldots, Q$, $Q_1, Q_2, \ldots$; a set of agent constants $i, i_1, i_2, \ldots$ $(i, i_l \in \{1, \ldots, n\})$; a set of knowledge operators $\mathbf{K}_1$, $\mathbf{K}_2, \ldots$, $\mathbf{K}_n$; the distributed knowledge operator $\mathbf{D}$; the set of logical connectives $\supset$, $\wedge$, $\vee$, $\neg$.

Formulas are defined in traditional way from propositional symbols using logical connectives, knowledge operators $\mathbf{K}_i$, $i \in \{1, \ldots, n\}$, and distributed knowledge operator $\mathbf{D}$. An *atomic formula* is defined as any propositional symbol. Each formula different from atomic formula is called a *non-atomic* one. A formula of the shape $\mathbf{Q}A$ $(\mathbf{Q} \in \{\mathbf{K}_i, \mathbf{D}\})$ is called a *modal one*.

The formula $\mathbf{K}_iA$ means "*agent i knows A*". The formula $\mathbf{D}A$ means "*A is distributed knowledge of all set (group) of agents*". Distributed knowledge is the knowledge that is implicitly present in a group of agents, and which might become explicit if the agents were able to communicate. For instance, it is possible that no agent knows the assertion Q, while at the same time $\mathbf{D}Q$ may be derived from $\mathbf{K}_1P \wedge \mathbf{K}_2(P \supset Q)$. We have distributed knowledge of Q if, *putting our knowledge together*, *Q may be deduced, even if none of us individually knows Q*.

Knowledge operators $\mathbf{K}_i$, $i \in \{1, \ldots, n\}$, and distributed knowledge operator $\mathbf{D}$ for the logic $S4_nD$ satisfy relations which comply with reflexivity and transitivity properties. The semantics of knowledge operators $\mathbf{K}_i$ and distributed knowledge operator $\mathbf{D}$ is defined using Kripke structure (see, e.g., (Fagin and Vardi, 1986; Fagin *et al.*, 1992; Halpern and Moses, 1992; Fagin *et al.*, 1995; Meyer and van der Hoek, 1995)). Let us remind the semantics of the formulas $\mathbf{K}_iA$ and $\mathbf{D}A$. Let S be a set of "states", s, t be some states from S, Π be an interpretation function, R_i $(i \in \{1, \ldots, n\})$ be the possibility (accessibility) relations, satisfying reflexivity and transitivity properties. Then in Kripke structure $M = (S, \Pi, R_1, \ldots, R_n)$ $(M, s) \models \mathbf{K}_iA$ iff $(M, t) \models A$ for all t such that $(s, t) \in R_i$; $(M, s) \models \mathbf{D}A$ iff $(M, t) \models A$ for all t such that $(s, t) \in R_1 \cap \ldots \cap R_n$. Following (Fagin *et al.*, 1992) the intuition behind the definition of semantics of the formula $\mathbf{D}A$ is that if all the agents could "combine their knowledge" the only worlds they would consider possible are precisely those in the intersection of the set of worlds that each one individually considers possible.

A Hilbert-style calculus $HS4_nD$ for the logic $S4_nD$ is defined by the following postulates:

Axioms for logical connectives $\supset$, $\wedge$, $\vee$, $\neg$ (see, e.g., (Fitting, 1996)).

Axioms for knowledge operators $\mathbf{K}_i$ and distributed knowledge operator $\mathbf{D}$ (see, e.g., (Fagin *et al.*, 1995; Meyer and van der Hoek, 1995)):

$$\begin{array}{ll} \mathbf{K}_i A \wedge \mathbf{K}_i(A \supset B) \supset \mathbf{K}_i B \quad (1), & \mathbf{D}A \wedge \mathbf{D}(A \supset B) \supset \mathbf{D}B \quad (2), \\ \mathbf{K}_i A \supset A \quad (3), & \mathbf{D}A \supset A \quad (4), \\ \mathbf{K}_i A \supset \mathbf{K}_i \mathbf{K}_i A \quad (5), & \mathbf{D}A \supset \mathbf{D}\mathbf{D}A \quad (6), \end{array}$$

$$\mathbf{K}_i A \supset \mathbf{D}A \quad (i = 1, \dots, n) \quad (7).$$

Rules:

$$\frac{A, A \supset B}{B}\,(R1) \qquad \frac{A}{\mathbf{K}_i A}\,(R2) \qquad \frac{A}{\mathbf{D}A}\,(R3).$$

The axioms (1) and (2) are the distributivity axioms for the operators $\mathbf{K}_i$ and $\mathbf{D}$; the axioms (3) and (4) are the reflexivity axioms for the operators $\mathbf{K}_i$ and $\mathbf{D}$; the axioms (5) and (6) are the transitivity axioms for the operators $\mathbf{K}_i$ and $\mathbf{D}$; the axiom (7) is the interaction axiom between the operators $\mathbf{K}_i$ and $\mathbf{D}$.

Thus knowledge operators $\mathbf{K}_i$ (distributed knowledge operator $\mathbf{D}$) satisfy the postulates of the multi-modal logic $S4_n$ (modal logic $S4$, respectively). In (Fagin *et al.*, 1992; Halpern and Moses, 1992; Fagin *et al.*, 1995; Meyer and van der Hoek, 1995) soundness and completeness of the calculus $HS4_nD$ are proved. A finite model property, i.e., decidability of $S4_nD$ is also proved in (Fagin *et al.*, 1995).

In Gentzen-style calculus for the considered logic instead of formulas we consider sequents, i.e., formal expressions $A_1, \dots, A_k \to B_1, \dots, B_m$ where $A_1, \dots, A_k$ $(B_1, \dots, B_m)$ is a multiset of formulas. A sequent is interpreted as a formula $\bigwedge_{i=1}^{k} A_i \supset \bigvee_{j=1}^{m} B_j$, $k, m \geqslant 0$. This formula is called a translation of the sequent S and denoted by $T(S)$.

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

Let G be some sequent calculus, and let i be any inference rule of the G. A rule (i) is applied to get the conclusion of (i) from the premises of (i). If a 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)". A rule (i) is *invertible* in G, if the derivability in G of the conclusion of (i) implies the derivability in G of each premise of (i). As usual, proof search in sequent calculi is implemented by applying the rules backwards. If a rule (i) is invertible, the backward application of (i) preserves the derivability. 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. A rule (i) is *admissible* rule in G, if adding (i) to the calculus G the set of derivable sequents in G is not extended.

Let us introduce a Gentzen-style calculus $GS4_nD$ for the logic $S4_nD$. The calculus $GS4_nD$ is defined by the following postulates:

Axiom: $\Gamma, P \to \Delta, P$ where P is an atomic formula.

Logical rules: traditional invertible rules for logical connectives $\supset$, $\wedge$, $\vee$, $\neg$ (see, e.g., (Kanger, 1957; Gallier, 1986; Goré, 1999)).

Modal rules (rules for knowledge operators $\mathbf{K}_i$ and distributed knowledge operator $\mathbf{D}$):

- **Reflexivity rules:**

$$\frac{\Pi, A,\, \mathbf{K}_i A \to \Delta}{\Pi,\, \mathbf{K}_i A \to \Delta}\,(\mathbf{K}_i \to) \qquad \frac{\Pi, A,\, \mathbf{D}A \to \Delta}{\Pi,\, \mathbf{D}A \to \Delta}\,(\mathbf{D} \to);$$

- **Transitivity rules:**

$$\frac{\Gamma,\, \mathbf{K}_i\Gamma \to A}{\Pi,\, \mathbf{K}_i\Gamma \to \Delta,\, \mathbf{K}_i A}\,(\mathbf{K}_i) \qquad \frac{\Gamma,\, \mathbf{D}\Gamma \to A}{\Pi,\, \mathbf{D}\Gamma \to \Delta,\, \mathbf{D}A}\,(\mathbf{D}),$$

where $\mathbf{Q}\Gamma$ ($\mathbf{Q} \in \{\mathbf{K}_i,\, \mathbf{D}\}$) means either empty word or multiset of formulas $\mathbf{Q}A_1, \dots, \mathbf{Q}A_n$ ($n \geqslant 1$);

- **Interaction rule:**

$$\frac{\Gamma \to A}{\Pi,\, \mathbf{K}\Gamma \to \Delta,\, \mathbf{D}A}\,(I),$$

where $\mathbf{K}\Gamma$ means either empty word or multiset of formulas $\mathbf{K}_1 A_{1,1}, \dots, \mathbf{K}_1 A_{1,l1}, \dots, \mathbf{K}_n A_{n,1}, \dots, \mathbf{K}_n A_{n,ln}$, ($n \geqslant 1$).

Formula $\mathbf{Q}A$ ($\mathbf{Q} \in \{\mathbf{K}_i,\, \mathbf{D}\}$) is the *main* formula of the rules ($\mathbf{Q} \to$), ($\mathbf{Q}$), and (I). Formulas from $\mathbf{Q}\Gamma$ ($\mathbf{K}\Gamma$) are *additional main* formulas of the rules ($\mathbf{Q}$) where $\mathbf{Q} \in \{\mathbf{K}_i,\, \mathbf{D}\}$ ((I), correspondingly).

EXAMPLE 1. Let us demonstrate an application of the rule (I):

$$\frac{A, B, C \to M}{P,\, \mathbf{K}_1 A,\, \mathbf{K}_1 B,\, \mathbf{K}_3 C,\, \mathbf{D}E \to \mathbf{K}_4 N,\, \mathbf{D}M}\,(I)$$

By induction on the height of derivation we can prove

Lemma 1. *All logical rules and reflexivity rules* ($\mathbf{K}_i \to$) *and* ($\mathbf{D} \to$) *are invertible in* $GS4_nD$.

The rules ($\mathbf{K}_i$), ($\mathbf{D}$), and (I) are not invertible, in general. For example, backward applying ($\mathbf{K}_1$) to $\mathbf{K}_1 R$ in the sequent $\to \mathbf{K}_1 R,\, \mathbf{K}_2(P \vee \neg P)$ we get $\to R$ which is non-derivable, but backward applying ($\mathbf{K}_2$) to $\mathbf{K}_2(P \vee \neg P)$ we get a derivation. We can demonstrate the non-invertibility of the rules ($\mathbf{D}$) and (I) analogously.

Lemma 2. *For any sequent* S, $HS4_nD \vdash T(S)$ *if and only if* $GS4_nD \vdash S$.

The proof of Lemma 2 is presented in Appendix.

Using soundness and completeness of the calculus $HS4_nD$ and Lemma 2 we get

Theorem 1. *The calculus $GS4_nD$ is sound and complete.*

3. Specialization of the Reflexivity Rules

With a view to get stopping device different from loop checking let us introduce marked knowledge operators $\mathbf{K}_i^*$ and marked distributed knowledge operator $\mathbf{D}^*$ which allow us to get a specialization of derivations in which it is not possible to apply reflexive rules twice using the same occurrence of a formula as main formula.

Let G_1S4_nD be a calculus obtained from the calculus $GS4_nD$ by the following transformations:

• the axiom of G_1S4_nD has the same shape as the axiom of $GS4_nD$ but multiset Γ is permitted to contain some formulae of the shape $\mathbf{Q}^*B$ ($\mathbf{Q} \in \{\mathbf{K}_i, \mathbf{D}\}$), i.e., operators $\mathbf{K}_i$ and $\mathbf{D}$ can be marked;

• replacing the reflexivity rules ($\mathbf{K}_i \rightarrow$) and ($\mathbf{D} \rightarrow$) by the following ones:

$$\frac{\Pi, A, \mathbf{K}_i^* A \rightarrow \Delta}{\Pi, \mathbf{K}_i A \rightarrow \Delta}\ (\mathbf{K}_i^* \rightarrow) \qquad \frac{\Pi, A, \mathbf{D}^* A \rightarrow \Delta}{\Pi, \mathbf{D} A \rightarrow \Delta}\ (\mathbf{D}^* \rightarrow),$$

where in the conclusion of the rules ($\mathbf{Q}^* \rightarrow$) ($\mathbf{Q} \in \{\mathbf{K}_i, \mathbf{D}\}$) the operator $\mathbf{Q}$ in the main formula $\mathbf{Q}A$ is not marked;

• replacing the rules ($\mathbf{K}_i$), ($\mathbf{D}$), and (I) by the following ones:

$$\frac{\Gamma, \mathbf{K}_i\Gamma \rightarrow A}{\Pi, \mathbf{K}_i\Gamma \rightarrow \Delta, \mathbf{K}_i A}\ (\mathbf{K}_i^*) \quad \frac{\Gamma, \mathbf{D}\Gamma \rightarrow A}{\Pi, \mathbf{D}\Gamma \rightarrow \Delta, \mathbf{D}A}\ (\mathbf{D}^*)$$

$$\frac{\Gamma \rightarrow A}{\Pi, \mathbf{K}\Gamma \rightarrow \Delta, \mathbf{D}A}\ (I^*),$$

where the rules ($\mathbf{K}_i^*$), ($\mathbf{D}^*$), and (I^*) have the same shape as the rules ($\mathbf{K}_i$), ($\mathbf{D}$), and (I), correspondingly but $\mathbf{Q}\Gamma$ ($\mathbf{Q} \in \{\mathbf{K}_i, \mathbf{D}, \mathbf{K}\}$) is permitted to contain some formulae of the shape $\mathbf{Q}^*B$, i.e., operator $\mathbf{Q}$ in additional main formulae can be marked.

Let us consider the admissibility of structural rules (see, e.g., (Gallier, 1986)).

Lemma 3 (admissibility of structural rules and cut rule). *The following structural rules* (*weakening, contraction, and cut rule*):

$$\frac{\Gamma \rightarrow \Delta}{\nabla, \Gamma \rightarrow \Delta, \Theta}\ (W),$$

$$\frac{\Gamma \rightarrow \Delta, A, A}{\Gamma \rightarrow \Delta, A}\ (\rightarrow C) \qquad \frac{A, A, \Gamma \rightarrow \Delta}{A, \Gamma \rightarrow \Delta}\ (C \rightarrow),$$

$$\frac{\Gamma \to \Delta, A;\ A, \Pi \to \Theta}{\Gamma, \Pi \to \Delta, \Theta}\ (cut),$$

are admissible in G where $G \in \{GS4_nD, G_1S4_nD\}$.

The proof of this lemma is presented in Appendix.

Using induction on the height of a derivation the invertibility of logical rules and the reflexivity rules $(\mathbf{K}_i^* \to)$ and $(\mathbf{D}^* \to)$ in G_1S4_nD can be proved.

From definition of the calculi $GS4_nD$ and G_1S4_nD we get

Lemma 4. *If $G_1S4_nD \vdash S$ then $GS4_nD \vdash S$, where a sequent S does not contain occurrences of marked operators.*

To justify specialization of reflexivity rules it is necessary to prove that for any sequent S not containing occurrences of marked operators from $GS4_nD \vdash S$ follows $G_1S4_nD \vdash S$. To this end let us introduce an auxiliary calculus $G_1^dS4_nD$. Let $G_1^dS4_nD$ be a calculus obtained from the calculus G_1S4_nD adding the following rules:

$$\frac{\Pi, A,\ \mathbf{K}_i^*A \to \Delta}{\Pi,\ \mathbf{K}_i^*A \to \Delta}\ (\mathbf{K}_i^{*d} \to) \qquad \frac{\Pi, A,\ \mathbf{D}^*A \to \Delta}{\Pi,\ \mathbf{D}^*A \to \Delta}\ (\mathbf{D}^{*d} \to).$$

It is obvious that if a sequent S does not contain occurrences of marked operators and $GS4_nD \vdash S$ then $G_1^dS4_nD \vdash S$. To prove that if $GS4_nD \vdash S$ then $G_1S4_nD \vdash S$ it is sufficient to prove that the rules $(\mathbf{K}_i^{*d} \to)$ and $(\mathbf{D}^{*d} \to)$ are admissible in G_1S4_nD.

Lemma 5. *The rules $(\mathbf{K}_i^{*d} \to)$, $(\mathbf{D}^{*d} \to)$ are admissible in G_1S4_nD.*

The proof of this lemma is presented in Appendix.

From Lemma 5 it follows

Lemma 6. *If $GS4_nD \vdash S$ then $G_1S4_nD \vdash S$.*

From Lemmas 4, 6 we get

Lemma 7. *$GS4_nD \vdash S$ if and only if $G_1S4_nD \vdash S$ where a sequent S does not contain occurrences of marked operators.*

Let us note that in the calculus G_1S4_nD applications of the reflexivity rules $(\mathbf{K}_i^* \to)$ and $(\mathbf{D}^* \to)$ are restricted in such way that it is not possible to apply these rules twice using the same occurrence of a formula as main formula.

4. Existential Invertibility of the Transitivity and Interaction Rules

First let us introduce the sequent calculus G_2S4_nD in which the rules $(\mathbf{D}^*)$ and (I^*) are combined into one rule. The calculus G_2S4_nD is obtained from the calculus G_1S4_nD

replacing the rules $(\mathbf{D}^*)$ and (I^*) by the following rule (named *combined interaction rule*):

$$\frac{\Gamma_1, \Gamma_2,\, \mathbf{D}\Gamma_2 \to A}{\Pi,\, \mathbf{K}\Gamma_1,\, \mathbf{D}\Gamma_2 \to \Delta,\, \mathbf{D}A}(I_c^*),$$

where $\mathbf{K}\Gamma_1$ $(\mathbf{D}\Gamma_2)$ means the same as in the rule (I) $((\mathbf{D})$, correspondingly). The formula $\mathbf{D}A$ is the main formula and formulas from $\mathbf{K}\Gamma_1$, $\mathbf{D}\Gamma_2$ are additional main formulas of the rule (I_c^*).

EXAMPLE 2. Let us demonstrate applications of the rules $(\mathbf{K}_i^*)$ and (I_c^*):

$$\frac{A,\, \mathbf{K}_1 A, B,\, \mathbf{K}_1^* B \to N}{P,\, \mathbf{K}_1 A,\, \mathbf{K}_1^* B,\, \mathbf{K}_3 C,\, \mathbf{D}E \to R,\, \mathbf{K}_1 N,\, \mathbf{D}M}\ (\mathbf{K}_1^*),$$

$$\frac{A, B, C, E,\, \mathbf{D}E \to M}{P,\, \mathbf{K}_1 A,\, \mathbf{K}_1^* B,\, \mathbf{K}_3 C,\, \mathbf{D}E \to R,\, \mathbf{K}_1 N,\, \mathbf{D}M}(I_c^*).$$

From the fact that the rules $(\mathbf{D}^*)$ and (I^*) are special cases of the rule (I_c^*) we get

Lemma 8. *If $G_1 S4_n D \vdash S$ then $G_2 S4_n D \vdash S$ where a sequent S does not contain occurrences of marked operators.*

Lemma 9. *The rule (I_c^*) is admissible in $G_1 S4_n D$.*

Proof. Let $G_1 S4_n D \vdash \Gamma_1, \Gamma_2,\, \mathbf{D}\Gamma_2 \to A$. Then using admissibility of weakening we get $G_1 S4_n D \vdash \Gamma_1,\, \mathbf{D}\Gamma_1, \Gamma_2,\, \mathbf{D}\Gamma_2 \to A$. Applying (D^*) to $\Gamma_1,\, \mathbf{D}\Gamma_1, \Gamma_2,\, \mathbf{D}\Gamma_2 \to A$ we get $G_1 S4_n D \vdash S = \Pi,\, \mathbf{D}\Gamma_1,\, \mathbf{D}\Gamma_2 \to \Delta,\, \mathbf{D}A$. Let $\Gamma_1 = A_1, \dots, A_n$ $(n \geqslant 1)$, then $\mathbf{D}\Gamma_1 = \mathbf{D}A_1, \dots,\, \mathbf{D}A_n$. It is obvious that $G_1 S4_n D \vdash S_i = A_i \to A_i$. Applying the rule (I^*) to S_i we get $G_1 S4_n D \vdash S_i^* = \mathbf{K}_i A_i \to \mathbf{D}A_i$. Starting from a sequent S and using S_i^* and cut rule (and relying on admissibility of cut rule) we get $G_1 S4_n D \vdash \Pi,\, \mathbf{K}\Gamma_1,\, \mathbf{D}\Gamma_2 \to \Delta,\, \mathbf{D}A$.

From Lemmas 8, 9 we get

Lemma 10. *$G_1 S4_n D \vdash S$ if and only if $G_2 S4_n D \vdash S$ where a sequent S does not contain occurrences of marked operators.*

It is easy to see that the combined interaction rule (I_c^*) as well as the rule $(\mathbf{K}_i^*)$ is not invertible. To get existential invertibility of the transitivity rule $(\mathbf{K}_i^*)$ and rule (I_c^*) let us introduce some canonical form of sequents.

A sequent S is a *primary* one, if S is of the following shape:

$\Sigma_1,\, \mathbf{K}^*\Gamma_1,\, \mathbf{D}^*\Pi_1 \to \Sigma_2,\, \mathbf{K}\Gamma_2,\, \mathbf{D}\Pi_2$, where

- Σ_i $(i \in \{1, 2\})$ is empty or consists of propositional symbols;
- $\mathbf{K}^*\Gamma_1$ is empty or consists of formulas of the shape $\mathbf{K}_l^* B$;

- $\mathbf{D}^*\Pi_1$ is empty or consists of formulas of the shape $\mathbf{D}^*B$;
- $\mathbf{K}\Gamma_2$ is empty or consists of formulas of the shape $\mathbf{K}_l A$;
- $\mathbf{D}\Pi_2$ is empty or consists of formulas of the shape $\mathbf{D}A$.

Lemma 11 (reduction to primary sequents). *Every sequent S can be reduced to a set of primary sequents $\{S_1, \dots, S_m\}$, $m \geqslant 1$, by applying the logical and reflexivity rules of G_2S4_nD backwards. Moreover, if $G_2S4_nD \vdash^V S$ then for all j $(j \in \{1, \dots, m\})$ $G_2S4_nD \vdash^{V_j} S_j$.*

Proof. Follows from invertibility of the logical and reflexivity rules.

Let G_3S4_nD be a calculus obtained from the calculus G_2S4_nD replacing the rules $(\mathbf{K}_i^*)$ and (I_c^*) by the following rules where the conclusion is a primary sequent and $\Sigma_1 \cap \Sigma_2$ is empty:

$$\frac{\Gamma_{1j}^\circ,\ \mathbf{K}_j^*\Gamma_{1j}^\circ \to\ A_i}{\Sigma_1,\ \mathbf{K}^*\Gamma_1,\ \mathbf{D}^*\Pi_1 \to \Sigma_2,\ \mathbf{K}\Gamma_2,\ \mathbf{K}_i A_i,\ \mathbf{D}\Pi_2}(\mathbf{K}_i^p),$$

where $\mathbf{K}^*\Gamma_1 = \mathbf{K}_1^*\Gamma_{11}, \dots, \mathbf{K}_n^*\Gamma_{1n}$ and $\mathbf{K}_j^*\Gamma_{1j} (j \in \{1, \dots, n\})$ is empty or consists of formulas of the shape $\mathbf{K}_j^*B$; $i \in \{1, \dots, m\}$, and if there exists $j (j \in \{1, \dots, n\})$ such that $i = j$ then $\Gamma_{1j}^\circ = \Gamma_{1i}$ else Γ_{1j}° and $\mathbf{K}_j^*\Gamma_{1j}^\circ$ are empty;

$$\frac{\Gamma_1, \Pi_1,\ \mathbf{D}^*\Pi_1 \to A}{\Sigma_1,\ \mathbf{K}^*\Gamma_1,\ \mathbf{D}^*\Pi_1 \to \Sigma_2,\ \mathbf{K}\Gamma_2,\ \mathbf{D}\Pi_2,\ \mathbf{D}A}(I_c^p).$$

A primary sequent of the shape $\Sigma_1,\ \mathbf{K}^*\Gamma,\ \mathbf{D}^*\Pi \to \Sigma_2$ where $\Sigma_1 \cap \Sigma_2$ is empty and $\mathbf{K}^*\Gamma$ $(\mathbf{D}^*\Pi)$ is empty or consist of formulas of the shape $\mathbf{K}_i^*M$ $(\mathbf{D}^*M$, correspondingly), is a *final* one. It is *impossible* to apply any rule to a final sequent.

Let us note that we start backward derivation in the calculus G_3S4_nD from a sequent not containing occurrences of marked operators.

A derivation V of a sequent S in the calculus G_3S4_nD is a *successful* one, if *each* branch of V ends with an axiom. A derivation V of S in the calculus G_3S4_nD is an *unsuccessful* one if V contains a branch ending with a final sequent. A sequent S is *derivable* in the calculus G_3S4_nD if and only if *there exists* a successful derivation V of S. Thus, if *all possible* derivations of S in G_3S4_nD are unsuccessful, the sequent S is *non-derivable*.

From definition of the calculi G_2S4_nD and G_3S4_nD we get

Lemma 12. *If $G_3S4_nD \vdash S$ then $G_2S4_nD \vdash S$.*

Using Lemma 11 we can prove

Lemma 13. *If $G_2S4_nD \vdash S$ then $G_3S4_nD \vdash S$.*

From Lemmas 12, 13 we get

Lemma 14. *$G_2S4_nD \vdash S$ if and only if $G_3S4_nD \vdash S$.*

Lemma 15 (existential invertibility of the rules $(\mathbf{K}_i^p)$ and (I_c^p)). *Let S be a primary sequent $\Sigma_1,\, \mathbf{K}^*\Gamma_1,\, \mathbf{D}^*\Pi_1 \;\rightarrow\; \Sigma_2,\, \mathbf{K}\Gamma_2,\, \mathbf{D}\Pi_2$ such that $\Sigma_1 \cap \Sigma_2$ is empty. Let $G_3S4_nD \vdash S$, then*

- *there exists a formula $\mathbf{K}_iA_i$ from $\mathbf{K}\Gamma_2$ such that $G_3S4_nD \vdash \Gamma^\circ_{1j},\, \mathbf{K}^*_j\Gamma^\circ_{1j} \rightarrow A_i$, where $\Gamma^\circ_{1j} = \Gamma_{1i}$ if $j = i$, otherwise Γ°_{1j} and $\mathbf{K}^*_j\Gamma^\circ_{1j}$ are empty; or*
- *there exists a formula $\mathbf{D}A$ from $\mathbf{D}\Pi_2$ such that $G_3S4_nD \vdash \Gamma_1, \Pi_1,\, \mathbf{D}^*\Pi_1 \rightarrow A$.*

Proof. The proof is carried out by induction on the height of the given derivation of the sequent S.

Lemma 15 allows us to restrict backtracking in backward proof search in G_3S4_nD.

Using Lemmas 7, 10, 14, and relying on soundness and completeness of initial calculus $GS4_nD$ (Theorem 1) we get

Theorem 2. *The calculus G_3S4_nD is sound and complete.*

5. Termination of Derivations in G_3S4_nD

If *loop-check is not used* backward proof search in G_3S4_nD *does not terminate*, in general.

EXAMPLE 3. Let S be the sequent $\mathbf{K}_1\neg\,\mathbf{K}_1\neg\,\mathbf{K}_1\neg\,\mathbf{K}_1\neg P \;\;\rightarrow$. Let A denotes $\mathbf{K}_1\neg\,\mathbf{K}_1\neg\,\mathbf{K}_1\neg P$, then the considered sequent S is $\mathbf{K}_1\neg A \rightarrow$. The derivation of the S in G_3S4_nD does not terminate.

$$\begin{array}{cl}
S_5 = \mathbf{K}_1^*\neg A,\, \mathbf{K}_1^*\neg\,\mathbf{K}_1\neg P,\, \mathbf{K}_1^*\neg\,\mathbf{K}_1\neg P \rightarrow A,\, \mathbf{K}_1\neg P & \\
\hline
S_4 = \mathbf{K}_1^*\neg A,\, \mathbf{K}_1^*\neg\,\mathbf{K}_1\neg P, P \rightarrow A,\, \mathbf{K}_1\neg P & (\mathbf{K}_1^p), (\neg \rightarrow \neg), (\mathbf{K}_1^* \rightarrow) \\
\hline
S_3 = \mathbf{K}_1^*\neg A,\, \mathbf{K}_1^*\neg\,\mathbf{K}_1\neg P \rightarrow A,\, \mathbf{K}_1\neg P & (\mathbf{K}_1^p), (\neg \rightarrow \neg) \\
\hline
S_2 = \mathbf{K}_1^*\neg A,\, \mathbf{K}_1\neg\,\mathbf{K}_1\neg P \rightarrow A & (\mathbf{K}_1^* \rightarrow), (\neg \rightarrow) \\
\hline
S_1 = \mathbf{K}_1^*\neg A \rightarrow A & (\mathbf{K}_1^p), (\neg \rightarrow \neg) \\
\hline
S = \mathbf{K}_1\neg A \rightarrow & (\mathbf{K}_1^* \rightarrow), (\neg \rightarrow)
\end{array}$$

where $(\neg\ \rightarrow\ \neg)$ denotes applications of two rules: $(\rightarrow\ \neg)$ and $(\neg\ \rightarrow)$. Let us note that the sequent S_5 is obtained from S_4 backward applying the rule $(\mathbf{K}_1^p)$ with A as the main formula. Since the sequent S_5 (up to application of contraction) coincides with S_3, continuing the derivation we again get the same sequent but we do not get a final sequent. Backward applying the rule $(\mathbf{K}_1^p)$ to S_4 with $\mathbf{K}_1\neg P$ as the main formula and rules $(\rightarrow \neg)$, $(\neg \rightarrow)$ we obtain the sequent $S_5^* = \mathbf{K}_1^*\neg A,\, \mathbf{K}_1^*\neg\,\mathbf{K}_1\neg P, P \rightarrow A,\, \mathbf{K}_1\neg P$ which coincides with S_4. Thus, constructing derivation in the calculus G_3S4_nD we can not avoid loop checking.

We now consider a safety fragment of the presented transitive distributed knowledge logic such that termination of derivations in this fragment can be established without loop-check. The considered fragment can be applied for specification and verification of *safety properties* of knowledge-based distributed systems (see, e.g., (Halpern, 1987; Fagin *et al.*, 1997; Huth and Ryan, 2000; Yoshioka *et al.*, 2001)). This safety fragment is defined by means of a restriction on positive occurrences of knowledge and distributed knowledge operators.

A positive occurrence of operator $\mathbf{Q}$ ($\mathbf{Q} \in \{\mathbf{K}_i, \mathbf{D}\}$) in a sequent S is a *special* one if it occurs within the scope of a negative occurrence of operator $\mathbf{Q}$ ($\mathbf{Q} \in \{\mathbf{K}_i, \mathbf{D}\}$) in S. A sequent S is a *safety* one if it does not contain special occurrences of operators $\mathbf{K}_i$, $\mathbf{D}$.

EXAMPLE 4. Let $S_1 = \mathbf{K}_1 \neg\, \mathbf{D} P \to$, $S_2 = \mathbf{D} \neg\, \mathbf{K}_2 P \to$, and $S_3 = \mathbf{K}_1\, \mathbf{D} P \to\ \mathbf{K}_1\, \mathbf{K}_2 P$. Then occurrences of operator $\mathbf{D}$ in S_1 and operator $\mathbf{K}_2$ in S_2 are special ones and the sequent S_3 does not contain special occurrences of operators $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{D}$. So, the sequent S_3 is safety.

Let B be a formula entering in a sequent S. A subformula of B is a *modal* one if it has the shape $\mathbf{Q}^{\mu} M$ where $\mathbf{Q} \in \{\mathbf{K}_i, \mathbf{D}\}$ and $\mu \in \{\varnothing, *\}$. A modal subformula $\mathbf{Q}^{\mu} M$ may occur both positively and negatively in B. The *complexity* of safety sequent S (denoted by $C(S)$) is defined as an ordered triple $< k(S), n(S), l(S) >$ where

- $k(S)$ is the number of *different modal subformulas* of the shape $\mathbf{Q}M$ ($\mathbf{Q} \in \{\mathbf{K}_i, \mathbf{D}\}$) entering in S *positively*;
- $n(S)$ is the number of *different modal subformulas* of the shape $\mathbf{Q}M$ (i.e., the outmost operator in $\mathbf{Q}M$ is not marked) entering in S and such that at least one occurrence of $\mathbf{Q}M$ enters in S *negatively* and *does not occur within the scope of marked operator* $\mathbf{Q}^*$ ($\mathbf{Q} \in \{\mathbf{K}_i, \mathbf{D}\}$ (it means that if a considered modal subformula enters in S negatively and occurs *only* within the scope of marked operators then this subformula is not counted);
- $l(S)$ is the length of S defined as $\sum_{i=1}^{k} l(B_i)$, where $l(B_i)$ is the length (defined in a traditional way) of i-th ($1 \leqslant i \leqslant k$) member of a sequent S.

Lemma 16. *Let $G_3S4_nD \vdash^V S^*$, and (j) is a rule of the calculus G_3S4_nD. Let a safety sequent S be a conclusion of an application of the rule (j) in V and S_1 be a premise of the same application of the rule (j). Then $C(S_1) < C(S)$.*

Proof. If (j) is a logical rule then $k(S_1) \leqslant k(S)$, $n(S_1) \leqslant n(S)$ but $l(S_1) < l(S)$. If $(j) = (\mathbf{Q}^* \to)$ $(\mathbf{Q}^* \in \{\mathbf{K}_i^*, \mathbf{D}^*\})$ then $n(S_1) < n(S)$. If $(j) = (\mathbf{Q}^p)$ $(\mathbf{Q}^p \in \{\mathbf{K}_i^p, I_c^p\}$ then $k(S_1) < k(S)$. Thus, in all cases $C(S_1) < C(S)$.

EXAMPLE 5. Derivations constructed below demonstrate a backward proof search in G_3S4_nD. We can check that the derivations terminate and the complexity of the safety sequents in backward derivation decreases.

(a) Let S be a sequent $\mathbf{K}_1\mathbf{K}_2P \rightarrow \mathbf{K}_1R$. Then unsuccessful derivation of S in G_3S4_nD is the following:

$$\begin{array}{c l}
S_4 = P,\, \mathbf{K}_2^*P,\, \mathbf{K}_1^*\mathbf{K}_2P \rightarrow R & \\ \hline
S_3 = \mathbf{K}_2P,\, \mathbf{K}_1^*\mathbf{K}_2P \rightarrow R & (\mathbf{K}_2^* \rightarrow) \\ \hline
S_2 = P,\, \mathbf{K}_2^*P,\, \mathbf{K}_1^*\mathbf{K}_2P \rightarrow \mathbf{K}_1R & (\mathbf{K}_1^p) \\ \hline
S_1 = \mathbf{K}_2P,\, \mathbf{K}_1^*\mathbf{K}_2P \rightarrow \mathbf{K}_1R & (\mathbf{K}_2^* \rightarrow) \\ \hline
S = \mathbf{K}_1\mathbf{K}_2P \rightarrow \mathbf{K}_1R & (\mathbf{K}_1^* \rightarrow)
\end{array}$$

Since the sequent S_4 is a final sequent and the presented derivation is the only possible, $G_3S4_nD \nvdash S$.

Let us evaluate the complexity of each sequent in the derivation constructed: $C(S) =< 1, 2, 5 >$, $C(S_1) =< 1, 1, 7 >$, $C(S_2) =< 1, 0, 8 >$, $C(S_3) =< 0, 1, 6 >$, $C(S_4) =< 0, 0, 7 >$; thus, $C(S_4) < C(S_3) < C(S_2) < C(S_1) < C(S)$.

(b) Let S be a sequent $\mathbf{K}_1\mathbf{K}_2P \rightarrow \mathbf{K}_1\mathbf{D}P, \mathbf{D}R$. We can construct the following successful derivation of S in G_3S4_nD:

$$\begin{array}{c l}
S_5 = P,\, \mathbf{K}_2P \rightarrow P & \\ \hline
S_4 = P,\, \mathbf{K}_2^*P,\, \mathbf{K}_1^*\mathbf{K}_2P \rightarrow \mathbf{D}P & (I_c^p) \\ \hline
S_3 = \mathbf{K}_2P,\, \mathbf{K}_1^*\mathbf{K}_2P \rightarrow \mathbf{D}P & (\mathbf{K}_2^* \rightarrow) \\ \hline
S_2 = P,\, \mathbf{K}_2^*P,\, \mathbf{K}_1^*\mathbf{K}_2P \rightarrow \mathbf{K}_1\mathbf{D}P,\, \mathbf{D}R & (\mathbf{K}_1^p) \\ \hline
S_1 = \mathbf{K}_2P,\, \mathbf{K}_1^*\mathbf{K}_2P \rightarrow \mathbf{K}_1\mathbf{D}P,\, \mathbf{D}R & (\mathbf{K}_2^* \rightarrow) \\ \hline
S = \mathbf{K}_1\mathbf{K}_2P \rightarrow \mathbf{K}_1\mathbf{D}P,\, \mathbf{D}R & (\mathbf{K}_1^* \rightarrow)
\end{array}$$

The sequent S_5 is an axiom. $C(S) =< 3, 2, 8 >$, $C(S_1) =< 3, 1, 10 >$, $C(S_2) = < 3, 0, 11 >$, $C(S_3) =< 1, 1, 7 >$, $C(S_4) =< 1, 0, 8 >$, $C(S_5) =< 0, 1, 4 >$; thus, $C(S_5) < C(S_4) < C(S_3) < C(S_2) < C(S_1) < C(S)$.

Remark 1. Relying on definition of $C(S)$ we get PSPACE complexity of the procedure to determine a termination of backward derivations of a safety sequent S^*. For every safety sequent S from a constructed derivation of a given sequent S^* we have $c^2k(S) + cn(S) + l(S)$, where $c = l(S^*)$. PSPACE complexity for mono-modal $S4$ presented in (Heuerding *et al.*, 1996) depends on lengths of components sequent with two halves and history. In (Ladner, 1977) PSPACE complexity for propositional mono-modal logics including $S4$ is obtained relying on Gentzen-like calculus with loop-checking. Propositional mono-modal logics correspond to one agent knowledge logics. In (Halpern and Moses, 1992), Ladner results from (Ladner, 1977) were extended to many agents and common knowledge logics.

Relying on the calculus G_3S4_nD, definition of derivability in G_3S4_nD, Lemmas 11, 15, 16, and using invertibility of the logical rules and reflexivity rules we get loop-check-free PSPACE procedure with restricted backtracking to determine a termination for backward proof search of a safety sequent. The procedure consists of several levels. Each level contains three main parts:

- the considered safety sequent S is reduced to a set of primary sequents;
- the obtained set of primary sequents is checked. If the considered primary sequent is an axiom then the considered branch of derivation is finished and a derivation of the next primary sequent is constructed;
- if the considered primary sequent is not an axiom then, according to Lemma 15, rules $(\mathbf{K}_i^p)$ and (I_c^p) are backward applied (in all possible ways). The premise of this application is used to start a new level of algorithm.

Thus a derivation in G_3S4_nD consists of repeating reductions to primary sequents and following backward application of one-in-two rules $(\mathbf{K}_i^p)$, (I_c^p) to each received primary sequent. It is obvious that algorithm finishes a search when either in all branches an axiom is obtained or a final sequent is obtained in all possible derivations. This algorithm does not use loop-check. Termination of the algorithm follows from Lemma 16.

6. Conclusions and Further Investigations

In the paper the transitive distributed knowledge logic is considered. For the safety fragment of this logic the new method to determine a termination of derivations is presented. The method is based on the sequent calculus and exploits marked knowledge and distributed knowledge operators. The marked operators and the rules corresponding to knowledge and distributed knowledge operators allow us to obtain termination of derivations in the considered safety fragment of the transitive distributed knowledge logic. By relying on the constructed loop-check-free sequent calculus a PSPACE decision procedure for the safety fragment of the considered logic is presented.

The following research looks promising:

- application of deduction-based methods for specification and verification of knowledge-based distributed systems;
- investigation of various knowledge-based (including common knowledge) logics with the aim to obtain effective tools allowing to determine a termination of derivations.

Appendix

In the Appendix proofs of Lemma 2 (Section 2) and Lemmas 3 and 5 (Section 3) are presented.

We now prove Lemma 3 for the calculus $GS4_nD$. For the calculus G_1S4_nD Lemma 3 can be proved in just the same way as for $GS4_nD$. The proof of Lemma 3 is carried out by splitting this lemma to several separate lemmas.

Lemma 17 (admissibility of structural rule of weakening). *The structural rule of weakening*

$$\frac{\Gamma \to \Delta}{\nabla, \Gamma \to \Delta, \Theta}\,(W)$$

is admissible in $GS4_nD$.

Proof. Let $GS4_nD + (W)$ be a calculus obtained from the calculus $GS4_nD$ by adding structural rule of weakening. Let us prove the following

PROPOSITION 1. Let $GS4_nD + (W) \vdash^V S$. Let the last step in derivation V be the application of the rule (W), and V^* is a derivation of the premise of the considered application of (W) in $GS4_nD$. Then $GS4_nD \vdash S$.

The proof of the proposition is carried out using induction on $h(V^*)$, i.e., the height of derivation of the premise $\Gamma \to \Delta$ of (W). Let $h(V^*) = 0$, i.e., the sequent $\Gamma \to \Delta$ is an axiom. Then the conclusion of (W), i.e., the sequent $\Pi\Gamma \to \Delta, \Theta$ is an axiom as well. Let $h(V^*) > 0$ and (j) is a rule applied last in V^*. Let us consider the following cases:

1. $(j) = (I)$:

$$\cfrac{\cfrac{\Gamma \to A}{\Pi,\, \mathbf{K}\Gamma \to \Delta,\, \mathbf{D}A}\,(I)}{\nabla, \Pi,\, \mathbf{K}\Gamma \to \Delta, \Theta,\, \mathbf{D}A}\,(W)$$

Then desired derivation has the following shape:

$$\frac{\Gamma \to A}{\nabla, \Pi,\, \mathbf{K}\Gamma \to \Delta, \Theta,\, \mathbf{D}A}\,(I)$$

2. $(j) \in \{(\mathbf{K}_i), (\mathbf{D})\}$; both these cases are considered analogously to the previous one;
3. (j) is any logical rule or a reflexivity rule, for example, $(j) = (\mathbf{K}_i \to)$:

$$\cfrac{\cfrac{\Pi, A,\, \mathbf{K}_i A \to \Delta}{\Pi,\, \mathbf{K}_i A \to \Delta}\,(\mathbf{K}_i \to)}{\nabla, \Pi,\, \mathbf{K}_i A \to \Delta, \Theta}\,(W)$$

By induction assumption we get $GS4_nD \vdash S^* = \nabla, \Pi, A,\, \mathbf{K}_i A \to \Delta, \Theta$. Applying $(\mathbf{K}_i \to)$ to S^* we get desired derivation.

Thus the proofs of Proposition 1 and admissibility of structural rule of weakening (W) in the calculus $GS4_nD$ are finished.

REMARK 2. The cases 1 and 2 in the proof of Proposition 1 demonstrate that the structural rule of weakening is incorporated in the rules $(\mathbf{K}_i)$, $(\mathbf{D})$, and (I).

Lemma 18 (admissibility of structural rules of contraction). *The structural rules of contraction*

$$\frac{\Gamma \to \Delta, A, A}{\Gamma \to \Delta, A}\,(\to C) \qquad \frac{A, A, \Gamma \to \Delta}{A, \Gamma \to \Delta}\,(C \to),$$

are admissible in $GS4_nD$.

Proof. Let $GS4_nD+(C \to)$ be a calculus obtained from the calculus $GS4_nD$ by adding the structural rule $(C \to)$. Let us prove the following

PROPOSITION 2. Let $GS4_nD + (C \to) \vdash^V S$. Let the last step in derivation V be the application of the rule $(C \to)$, and V^* is a derivation of the premise of the considered application of $(C \to)$ in $GS4_nD$. Then $GS4_nD \vdash^{V^{**}} S$, moreover $h(V^{**}) \leqslant h(V^*)$.

The proof of the proposition is carried out using induction on $h(V^*)$, i.e., the height of derivation of the premise $A, A, \Gamma \to \Delta$ of $(C \to)$. The case when $h(V^*) = 0$ is obvious. Let $h(V^*) > 0$ and (j) be a rule applied last in V^*. Let us consider only the following two cases.

1. $(j) = (\mathbf{K}_i \to)$ and the main formula of $(\mathbf{K}_i \to)$ coincides with an explicit occurrence of A, i.e., $A = \mathbf{K}_iM$:

$$\cfrac{\cfrac{\Pi, M, \mathbf{K}_iM, \mathbf{K}_iM \to \Delta}{\Pi, \mathbf{K}_iM, \mathbf{K}_iM \to \Delta}\,(\mathbf{K}_i \to)}{\Pi, \mathbf{K}_iM \to \Delta}\,(C \to)$$

   By induction assumption we get $GS4_nD \vdash S^* = \Pi, M, \mathbf{K}_iM \to \Delta$. Applying $(\mathbf{K}_i \to)$ to S^* we get desired derivation.

2. $(j) = (\mathbf{K}_i)$ and one from additional formulas of $(\mathbf{K}_i)$ coincides with an explicit occurrence of A, i.e., $A = \mathbf{K}_iM$:

$$\cfrac{\cfrac{M, M, \Gamma, \mathbf{K}_iM, \mathbf{K}_iM, \mathbf{K}_i\Gamma \to B}{\Pi, \mathbf{K}_iM, \mathbf{K}_iM, \mathbf{K}_i\Gamma \to \Delta, \mathbf{K}_iB}\,(\mathbf{K}_i)}{\Pi, \mathbf{K}_iM, \mathbf{K}_i\Gamma \to \Delta, \mathbf{K}_iB}\,(C \to)$$

Let the derivation of a sequent $M, M, \Gamma, \mathbf{K}_iM, \mathbf{K}_iM, \mathbf{K}_i\Gamma \to B$ is denoted by V'. By induction assumption we get $GS4_nD \vdash^{V'^*} M, M, \Gamma, \mathbf{K}_iM, \mathbf{K}_i\Gamma \to B$ and $h(V'^*) \leqslant h(V')$. It is obvious that $h(V') < h(V^*)$. Using induction assumption once more we get $GS4_nD \vdash S^* = M, \Gamma, \mathbf{K}_iM, \mathbf{K}_i\Gamma \to B$. Applying $(\mathbf{K}_i \to)$ to S^* we get desired derivation.

Other cases are considered analogously. Thus, the proofs of Proposition 2 and admissibility of structural rule $(C \to)$ in $GS4_nD$ are finished.

The admissibility of structural rule $(\to C)$ in $GS4_nD$ is proved analogously.

Lemma 19 (admissibility of cut rule). *The cut rule*

$$\frac{\Gamma \rightarrow \Delta, A;\ A, \Pi \rightarrow \Theta}{\Gamma, \Pi \rightarrow \Delta, \Theta}\ (cut),$$

is admissible in $GS4_nD$.

Proof. Let $GS4_nD + (cut)$ be a calculus obtained from the calculus $GS4_nD$ by adding the structural rule (cut). Let us prove the following

PROPOSITION 3. Let $GS4_nD + (cut) \vdash^V S$. Let the last step in derivation V be the application of (cut), and V_1 (V_2) is a derivation of the left (right, correspondingly) premise of the considered application (cut) in $GS4_nD$. Then $GS4_nD \vdash S$.

The proof of the proposition is carried out using double induction on $< g(A), h(V_1) + h(V_2) >$, where $g(A)$ is the length of the (cut) formula A, $h(V_i)(i \in \{1,2\})$ is the height of derivation V_i of the premise. The case when $h(V_i) = 0$ $(i \in \{1,2\})$ is obvious. Let $h(V_1) + h(V_2) > 0$ and (l_i) be a rule applied last in V_i. Let us consider the case when $(l_1) = (\mathbf{K}_i)$, $(l_2) = (\mathbf{K}_i \rightarrow)$, and the main formulas of $(\mathbf{K}_i)$ and $(\mathbf{K}_i \rightarrow)$ coincide with the (cut) formula A:

$$\frac{V_1 \left\{ \dfrac{\Gamma,\, \mathbf{K}_i\Gamma \rightarrow A}{\Pi,\, \mathbf{K}_i\Gamma \rightarrow \Delta,\, \mathbf{K}_iA}\,(\mathbf{K}_i)\right. ;\quad \dfrac{V_2'\,\{A,\, \mathbf{K}_iA, \nabla \rightarrow \Theta}{\mathbf{K}_iA, \nabla \rightarrow \Theta}\,(\mathbf{K}_i \rightarrow)}{\Pi,\, \mathbf{K}_i\Gamma, \nabla \rightarrow \Delta, \Theta}\,(cut)$$

Applying (cut) to sequents Π, $\mathbf{K}_i\Gamma \rightarrow \Delta$, $\mathbf{K}_iA$ and A, $\mathbf{K}_iA, \nabla \rightarrow \Theta$ and using induction on $h(V_1) + h(V_2')$ we get $GS4_nD \vdash \Pi,\, \mathbf{K}_i\Gamma, A, \nabla \rightarrow \Delta, \Theta$. Applying (cut) to sequents Γ, $\mathbf{K}_i\Gamma \rightarrow A$ and Π, $\mathbf{K}_i\Gamma, A, \nabla \rightarrow \Delta, \Theta$ and using induction on $g(A)$ and admissibility of contraction we get $GS4_nD \vdash S^* = \Gamma, \Pi,\, \mathbf{K}_i\Gamma, \nabla \rightarrow \Delta, \Theta$. Applying n time (where n is the number of members in Γ) the rule $(\mathbf{K}_i \rightarrow)$ from the sequent S^* we obtain the desired derivation of the sequent Π, $\mathbf{K}_i\Gamma, \nabla \rightarrow \Delta, \Theta$ in $GS4_nD$.

Other cases are considered analogously. Thus, Proposition 3 and admissibility of (cut) in $GS4_nD$ are proved.

Now let us prove an equivalence of the calculi $HS4_nD$ and $GS4_nD$.

Lemma 20. *Let S be a sequent $A_1, \ldots, A_n \rightarrow B_1, \ldots, B_m$ and $T(S) = \bigwedge_{i=1}^{n} A_i \supset \bigvee_{j=1}^{m} B_j$, $n, m \geqslant 0$. Let $HS4_nD \vdash^V T(S)$, then $GS4_nD \vdash S$.*

Proof. The proof is carried out using induction on $h(V)$. Let $h(V) = 0$, i.e., the formula $T(S)$ is an axiom. Let us consider only the case when $T(S)$ is an interaction axiom. Then desired derivation of this axiom is obtained using the rule (I). Let $h(V) > 0$ and the last step in the derivation of $T(S)$ is application of the rule $(Ri)(i \in \{1,2,3\})$. The case when $i = 1$ is considered using admissibility of (cut) in $GS4_nD$. Let $i = 2$, i.e., the rule $\frac{A}{\mathbf{K}_iA}$ (R2) was applied as the last step of the derivation. In this case, according to induction hypothesis we get $GS4_nD \vdash \rightarrow A$ and applying the rule $(\mathbf{K}_i)$ we get $GS4_nD \vdash \rightarrow \mathbf{K}_iA$. The case when $i = 3$ is considered analogously to previous case.

Let us prove the inverse lemma, i.e.,

Lemma 21. *Let $GS4_nD \vdash^V S$, then $HS4_nD \vdash T(S)$.*

Proof. The proof is carried out using induction on $h(V)$. Let us consider only the case when the last step in derivation V of the sequent S is the application of the rule (I):

$$\frac{\Gamma \rightarrow A}{\Pi,\, \mathbf{K}\Gamma \rightarrow \Delta,\, \mathbf{D}A}\ (I)$$

Let $\Gamma = A_1, \ldots, A_n$, then using induction hypothesis we get $HS4_nD \vdash \bigwedge_{i=1}^n A_i \supset A$ (1). Using the rule (R_3), distributivity axiom for the operator $\mathbf{D}$, and the fact that $HS4_nD \vdash \mathbf{D}(A \wedge B) \equiv \mathbf{D}A \wedge \mathbf{D}B$, from (1) we get $HS4_nD \vdash \bigwedge_{i=1}^n \mathbf{D}A_i \supset \mathbf{D}A$ (2).

Let us note that deduction theorem for the calculus $HS4_nD$ can be proved in the same way as for $HS4$ (see, e.g., (Hughes and Cresswell, 1968)). Using interaction axiom, properties of logical connectives, and deduction theorem from (2) we obtain the desired derivation in $HS4_nD$ of the formula $\bigwedge \Pi \wedge \bigwedge_{i=1}^n \mathbf{K}_iA_i \supset \bigvee \Delta \vee \mathbf{D}A$ where $\bigwedge \Pi$ $(\bigvee \Delta)$ means conjunction (disjunction, correspondingly) of formulas from Π (Δ, correspondingly).

Other cases are considered in a similar way.

Lemma 2, i.e., for any sequent S, $HS4_nD \vdash T(S)$ if and only if $GS4_nD \vdash S$, follows from Lemmas 20 and 21.

Now let us prove Lemma 5 (Section 3). Let us recall that we start backward derivation in the calculus G_1S4_nD from a sequent not containing occurrences of marked operators, i.e., an end-sequent of any derivation in the calculus G_1S4_nD is an arbitrary sequent without marked operators. With a view to prove the Lemma 5 let us establish the following two propositions.

PROPOSITION 4. The rule $(\mathbf{D}^{*d} \rightarrow)$ is admissible in G_1S4_nD.

Proof. Let $G_1^dS4_nD \vdash^V S$. The proof of lemma is carried out using induction on the number of applications of the rule $(\mathbf{D}^{*d} \rightarrow)$ in V denoted by $n(V)$. Let us consider the lowest application of the rule $(\mathbf{D}^{*d} \rightarrow)$ in V. Let $\mathbf{D}^*A$ be the main formula of this lowest application of the rule $(\mathbf{D}^{*d} \rightarrow)$. Let $S_1 = A, \mathbf{D}^*A, \Gamma \rightarrow \Delta$ be the premise of this lowest application of the rule $(\mathbf{D}^{*d} \rightarrow)$. Since the end-sequent S of V does not contain marked operator $\mathbf{D}^*$, below this lowest application must be an application of the rule $(\mathbf{D}^* \rightarrow)$ with the main formula $\mathbf{D}A$. Let $S_2 = A, \mathbf{D}^*A, \Pi \rightarrow \Theta$ be the premise of the considered application of the rule $(\mathbf{D}^* \rightarrow)$. Let V_1 be the part of V between the sequents S_1 and S_2. Let us consider the following cases:

1. The part V_1 does not contain an application of the rule $(\mathbf{D}^*)$. In this case let us drop the considered lowest application of the rule $(\mathbf{D}^{*d} \rightarrow)$ in V and leave fixed the applications of other rules in V_1. Instead of V_1 we get the part V_1^* with end-sequent $S_2^* = A, A,\ \mathbf{D}^*A, \Pi \rightarrow \Theta$. Relying on admissibility of the rule of contraction and applying the rule $(\mathbf{D}^* \rightarrow)$ from S_2^* we get the sequent $\mathbf{D}A, \Pi \rightarrow \Theta$. As a result we get V^+ instead of V such that $n(V^+) < n(V)$. So, by induction assumption we get $G_1S4_nD \vdash^{V^*} S$.
2. The part V_1 contains an application of the rule $(\mathbf{D}^*)$. Let us consider the topmost application of the rule $(\mathbf{D}^*)$ in V_1.

$$\frac{S_1' = A, \nabla,\ \mathbf{D}^*A,\ \mathbf{D}\nabla \rightarrow B}{S_1'' = \Omega_1,\ \mathbf{D}^*A,\ \mathbf{D}\nabla \rightarrow \Omega_2,\ \mathbf{D}B}\ (\mathbf{D}^*).$$

Let V_1' be the part of V_1 between the sequents S_1 (i.e., the premise of the lowest application of $(\mathbf{D}^{*d} \rightarrow)$) and S_1'. Let us drop the considered lowest application of the rule $(\mathbf{D}^{*d} \rightarrow)$ in V and leave fixed the applications of other rules in the part V_1'. Instead of V_1' we get the part with end-sequent $S_1^{'*} = A, A, \nabla,\ \mathbf{D}^*A,\ \mathbf{D}\nabla \rightarrow B$. Relying on admissibility of the rule of contraction and applying the rule $(\mathbf{D}^*)$ from $S_1^{'*}$ we get the same sequent $S_1'' = \Omega_1,\ \mathbf{D}^*A,\ \mathbf{D}\nabla \rightarrow \Omega_2,\ \mathbf{D}B$. As a result we get V^+ instead of V such that $n(V^+) < n(V)$. Therefore, by induction assumption we get $G_1S4_nD \vdash^{V^*} S$.

In the same way we can prove

PROPOSITION 5. The rule $(\mathbf{K}_i^{*d} \rightarrow)$ is admissible in G_1S4_nD.

References

Clarke, E., O. Grumberg and D. Peled (2000). *Model Checking*. MIT Press.

Cerrito, S., and M. Cialdea Mayer (1997). A polynomial translation of $S4$ into T and contraction-free tableaux for $S4$. *Journal of the Interest Gropup in Pure and Applied Logic*, **5**(2), 287–300.

Demri, S. (1995). Uniform and non uniform strategies for tableaux calculi for modal logics. *Journal of Applied Non-Classical Logics*, **5**(1), 77–96.

Dyckhoff, R. (1992). Contraction-free sequent calculi for intuitionistic logic. *Journal of Symbolic Logic*, **57**, 795–807.

Fagin, R., and M.Y. Vardi (1986). Knowledge and implicit knowledge in a distributed enviroment. In J.Y. Halpern (Ed.), *Proceedings of the 1st Conference on Theoretical Aspects of Knowledge*. Morgan Kaufmann, Los Altos. pp. 187–206.

Fagin, R., J.Y. Halpern and M.Y. Vardi (1992). What can machines know? On the properties of knowledge in distributed systems. *Journal of the ACM*, **39**(2), 328–376.

Fagin, R., J.Y. Halpern, Y. Moses and M.Y. Vardi (1995). *Reasoning about Knowledge*. MIT Press, Cambridge, Mass.

Fagin, R., J.Y. Halpern, Y. Moses and M.Y. Vardi (1997). Knowledge-based programs. *Distributed Computing*, **10**(4), 199–225.

Fitting, M. (1983). Proof methods for modal and intuitionistic logics. *Synthese Library*, **169**. D. Reidel Publishing Co., Dordrecht, Holland.

Fitting, M. (1993). Basic modal logic. In D.M. Gabbay, C.J. Hogger, J.A. Robinson (Eds.), *Handbook for Logic in Artificial Intelligence and Logic Programming. Logical Foundations*, vol. 1. pp. 365–447.

Fitting, M. (1996). *First-Order Logic and Automated Theorem Proving*, 2nd ed. Graduate texts in computer science. Springer-Verlag, New York Inc.

Gallier, J.H. (1986). *Logic for Computer Science, Foundations of Automatic Theorem Proving*. Harper Row, New York.

Goré, R. (1999). Chapter 6: Tableau methods for modal and temporal logics. In M. D'Agostino, D.M. Gabbay, R. Hähnle, J. Posegga (Eds.), *Handbook of Tableau Methods*. Kluwer Academic Publishers. pp. 297–396.

Halpern, J.Y. (1987). Using reasoning about knowledge to analyze didtributed systems. *Annual Review of Computer Science*, **2**, 37–68.

Halpern, J.Y., and Y. Moses (1992). A guide to completeness and complexity for modal logics of knowledge and belief. *Artificial Intelligence*, **54**(3), 319–379.

Heuerding, A., M. Seyfried and H. Zimmermann (1996). Efficient loop-check for backward proof search in some non-classical propositional logics. *Lecture Notes in Computer Science*, **1071**, 210–225.

Hudelmaier, J. (1992). Bounds for cut-elimination in intuitionistic propositional logic. *Arch. Math. Logic*, **31**, 331–353.

Hudelmaier, J. (1996). A contraction-free sequent calculus for $S4$. In H. Wansing (Ed.), *Proof Theory for Modal Logic*. Kluwer Academic Publishers, Dordrechts, Boston/London. pp. 3–16.

Hughes G.E., and M.J. Cresswell (1968). *An Introduction to Modal Logic*. Methuen & Co. Ltd, London.

Huth, M., and M. Ryan (2000). *Logic in Computer Science*: *Modeling and Reasoning about Systems*. Cambridge University Press.

Kanger, S. (1957). *Provability in Logic*. Almgvist & Wiksell, Stockholm.

Ladner, R. (1977). The computational complexity of provability in systems of modal propositional logic. *SIAM Journal of Computing*, **6**(3), 467–480.

Maslov, S.J. (1967). Invertible sequential variant of intuitionistic predicate calculus. *Zapiski Nauchnykh Seminarov V.A.Steklov Matemat. Institute Akademii Nauk SSSR*, (*LOMI*), **4**, 96–111.

Massacci, F. (2000). Single step tableaux for modal logics. *Journal of Automated Reasoning*, **24**(3), 319–364.

Meyer, J.J.Ch., and W. van der Hoek (1995). *Epistemic Logic for AI and Computer Science*. Cambridge University Press, Cambridge.

Pliuškevičius, R., and A. Pliuškevičienė (2004). Decision procedure for temporal logic of belief and actions. *Informatica*, **15**(3), 379–398.

Pliuškevičius,R., and A. Pliuškevičienė (2006). Decision procedure for a fragment of mutual belief logic with quantified agent variables. *Lecture Notes in Artificial Intelligence*, **3900**, 0112–0128.

Yoshioka, N., Y. Tahara, A. Ohsuga and S. Honiden (2001). Security for mobile agents. *Lecture Notes in Computer Science*, **1957**, 223–234.

R. Pliuškevičius, hab. doctor of mathematical sciences, associated professor, is a head of Mathematical Logic Department at the Institute of Mathematics and Informatics. He is a member of Lithuanian Mathematical Society and American Mathematical Society. His main research interests include computer-aided calculi for temporal logics, modal logics, agent-based and knowledge-based logics; loop-check-free and backtracking-free sequent calculi for non-classical logics.

A. Pliuškevičienė, doctor of mathematical sciences, associated professor, is a senior scientific researcher of Mathematical Logic Department at the Institute of Mathematics and Informatics. The field of research – proof theory of classical and non-classical logics including modal logics, temporal logics, agent-based and knowledge-based logics.

Išvedimų baigtinumas paskirstyto žinojimo tranzityvios logikos fragmentui

Regimantas PLIUŠKEVIČIUS, Aida PLIUŠKEVIČIENĖ

Nagrinėjama paskirstyto žinojimo logika, kurios bazė yra multi-modalinė logika $S4_n$. Tiriamas šios logikos fragmentas skirtas paskirstytų sistemų saugumo savybių verifikavimui. Nagrinėjamam fragmentui pateiktas išvedimo paieškos algoritmas, leidžiantis nustatyti išvedimų baigtinumą nenaudojant ciklų.