Theoretical Computer Science 536 (2014) 21–41

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

A framework for linear authorization logics

Vivek Nigam

Federal University of Paraíba, João Pessoa, Brazil

ARTICLE INFO

Article history:
Received 7 October 2012
Received in revised form 20 July 2013
Accepted 16 February 2014
Communicated by N. Shankar

Keywords:
Linear authorization logics
Logic complexity
Proof theory

ABSTRACT

Linear authorization logics (LALs) are logics based on linear logic that can be used for modeling effect-based authentication policies. LALs have been used in the context of the Proof-Carrying Authorization framework, where formal proofs must be constructed in order for a principal to gain access to some resource elsewhere. This paper investigates the complexity of the provability problem, that is, determining whether a formula is provable in a linear authorization logic. We show that the multiplicative propositional fragment of LAL is already undecidable in the presence of two principals. On the other hand, we also identify a first-order fragment of LAL for which provability is PSPACE-complete. Finally, we argue by example that the latter fragment is natural and can be used in practice.

1. Introduction

There are many situations where using and issuing authorizations may have effects. For example, a professor that is away might want to provide an authorization to one of his students to enter his office *at most once* in order to pick up a book. Once this student has consumed this authorization by entering the office, the student can no longer enter it unless he obtains another authorization.

Such a scenario has been implemented [7] following the Proof-Carrying Authorization (PCA) framework [6], where access control policies are specified as logical theories and whenever a principal (or agent) requests permission to access some resource, she provides a formal proof demonstrating that such an access follows from the policies. While the use of logic to specify access control policies dates back to some decades ago [2], the main difference between PCA and previous approaches is the existence of *proof objects*. The use of proof objects reduces the required trust base of the principals in a system, as a principal just needs to *check* whether the attached proof object is correct.

Access control logics for distributed systems are called *authorization logics* [4]. Traditionally classical logics have been used to specify policies. However, in order to specify *effect-based* policies, such as the one illustrated above, one moves to linear logic [20]. As linear logic formulas can be interpreted as resources, linear logic theories can model state-based systems and therefore are suitable for specifying policies that involve consumable credentials, such as money or the right to access a room at most once. *Linear authorization logics* (LAL) [18] are authorization logics based on linear logic extended with modality operators [4], e.g., $says$ or has.

A central requirement in PCA is the *construction* of proof objects from policies specified using (linear) authorization logics. Although it is easy to check whether a proof object is correct, finding a correct proof object involves proof search which may be hard. In PCA, it is the burden of the requesting principal, which is normally assumed to be more powerful, to construct such objects from the policies available. It is therefore important to determine how hard is the task of constructing proofs, that is, to determine the complexity of the *provability problem* for LAL.

E-mail address: vivek.nigam@gmail.com.

http://dx.doi.org/10.1016/j.tcs.2014.02.018
0304-3975/

The contributions of this paper are twofold: (1) we propose a logical framework for LAL and (2) we investigate the complexity of the provability problem for different fragments of LAL.

For our first contribution, we propose using the sequent calculus proof system SELL, introduced in [34], as a logical framework where one can specify different linear authorization logics. First, we show how to encode existing authorization logics [18]. Then we show how SELL allows one to specify a wider range of policies that did not seem possible before. For instance, we modularly increase the expressiveness of our encoding by showing that one can also express in SELL policies of the form: "A principal may use a lower-ranked set of policy rules, but not a higher-ranked set of policy rules."

Our second main contribution is of investigating the complexity of the provability problem for LAL. We show that the provability problem is *undecidable* already for the propositional multiplicative fragment with no function symbols and only two principals that have only consumable credentials. The proof follows by encoding a two-counter Minsky machine [31], which is known to be Turing complete. This means that constructing proof objects for simple policies may already not be computable. Interestingly, the upper bound for the provability problem for the same fragment (MELL) of linear logic [20] is not known. As exponentials can be seen as modalities, this result means that adding an extra modality to MELL leads in general to the undecidability of the resulting logic. This is in accordance with previous results on the complexity of SELL [9].

Our second complexity result is more interesting from both the application and technical points of view. In particular, we propose a *first-order* fragment of LAL for which the provability problem is PSPACE-complete with respect to the size of the given formula. In particular, we restrict policies to be only *balanced bipoles* with no function symbols and where principals have only consumable credentials, i.e., principals have credentials that can be used exactly once.

Bipoles is a class of logical formulas that often appear in proof theory literature [29]. From a proof search perspective, one can make precise connections (sound and complete correspondence) between the reachability problem of multiset rewriting systems (MSR) and the provability problem of linear logic bipoles [8,34]. However, the same correspondence does not work as smoothly when using LAL due to the presence of modalities, e.g., $says$. But as we show in this paper, it works when using the expressiveness gained by using SELL. In particular, we use the ability to specify in SELL when formulas should be proved *without* using any policy rules. That is, such a formula should be necessarily derived using only the set of already derived formulas. This condition can be intuitively interpreted as checking whether a formula follows from the state of the system (or table of a principal).

On the other hand, a sequence of papers [26,24,22,21] have investigated the complexity of the reachability problem for systems whose actions are *balanced*. An action is classified as balanced if its pre- and post-conditions have the *same number* of atomic formulas. It has been shown that the reachability problem for MSR with balanced actions is PSPACE-complete. Given the correspondence between the reachability and provability problem of bipoles formulas, we show that the provability problem for balanced bipoles is also PSPACE-complete.

This paper is structured as follows:

- Section 2 reviews the proof system SELL and the focused proof system for SELL, which is the machinery used to formally prove some of our theorems such as the correspondence between logic provability and MSR reachability.
- Section 3 shows how one can encode existing linear authorization logics and how to modularly extend such encoding in order to express a wider range of policies.
- Section 4 contains the undecidability proof for the propositional multiplicative fragment of the linear authorization logic proposed in [18].
- Section 5 describes the connections between bipoles and MSR, formalizing a novel correspondence between MSR reachability and logic provability of a first-order fragment of linear authorization logics, namely, when policies are bipoles.
- Section 6 contains the PSPACE-completeness proof for the provability problem when policies are balanced bipoles.
- Section 7 contains a student registration example based on a similar example from [18], but that is specified using balanced bipoles.

Finally, in Section 8 we conclude and comment on related work.

This is an expanded and improved version of the conference paper [33]. In particular, due to the suggestion of a reviewer, we simplified the encoding of LAL following the work of Pfenning and Davies [40]. Also, the encoding in [33] of Minsky machines used additive units ($\top$), thus not being purely multiplicative. Here, we modify that encoding and show that the purely multiplicative fragment of LAL (without $\top$) is undecidable.

2. A framework for linear authorization logics

We propose using linear logic with subexponentials (SELL) as a framework for specifying LAL. The system for classical linear logic with subexponentials was proposed in [11] and further investigated in [34]. However, as argued in [19], the use of intuitionistic logic seems more adequate to PCA applications as it allows only constructive proofs. We now review the proof system for intuitionistic linear logic with subexponentials in Section 2.1 and the focused proof system for this system, called SELLF, in Section 2.2.