On the Complexity of Linear Authorization Logics

Vivek Nigam
Ludwig-Maximilians-Universität, Munich, Germany
Email: vivek.nigam@ifi.lmu.de

***Abstract*—Linear authorization logics (LAL) are logics based on linear logic that can be used for modeling effect-based authentication policies. LAL has been used in the context of the Proof-Carrying Authorization framework, where formal proofs are 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 linear authorization logic formula is provable or not. 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.**

Keywords: Authorization Logics, Complexity, Linear Logic, Subexponentials

I. 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 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 [4] following the Proof-Carrying Authorization framework (PCA) [3], 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 [1], 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* [2]. 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 [15]. 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) [13] are authorization logics based on linear logic extended with modality operators [2], *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.

The contribution of this paper is 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 [23], as a logical framework where one can specify different linear authorization logics. First, we show how to encode existing authorization logics [13]. 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 [21], 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 [15] is not known. As exponentials can be seen as modalities, this result means that adding an extra modality to MELL possibly leads to undecidability.

Finally, 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 [20]. 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 [5], [23]. 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 recent papers [18], [17], [16] 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 II reviews the proof system SELL, showing 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 III contains the undecidability proof for the propositional multiplicative fragment of the linear authorization logic proposed in [13].
- Section IV describes the connections between bipoles and MSR, formalizing a novel correspondence between provability of a first-order fragment of linear authorization logics, namely, when policies are bipoles, and MSR reachability.
- Section V contains the PSPACE-completeness proof for the provability problem when policies are balanced bipoles.
- Section VI contains a student registration example based on a similar example from [13], but that is specified using balanced bipoles.

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

II. 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 [7] and further investigated in [23]. However, as argued in [14], 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.

Besides sharing all connectives with linear logic, SELL may include as many exponential-like connectives, called *subexponentials*, as one needs. Subexponentials, written $!^l$ and $?^l$, are labeled with an index, l. The subexponentials indexes available in a system are formally specified by the tuple $\langle I, \preceq, \mathcal{U} \rangle$, where I is the set of labels for subexponentials, $\preceq$ is a preorder relation among the elements of I, and $\mathcal{U} \subseteq I$ specifies which subexponentials allow weakening and contraction. The preorder $\preceq$, on the other hand, specifies the provability relation among subexponentials and is upwardly closed with respect to the set $\mathcal{U}$, *i.e.*, if $x \preceq y$ and $x \in \mathcal{U}$, then $y \in \mathcal{U}$.

Given a signature Σ, the proof system SELL_Σ is constructed as follows: The system contains all the introduction rules for $\&, \oplus, \otimes, \multimap, \exists, \forall$ and the units, $1, \top$ and 0 as well as the exchange rules exactly as in linear logic [15]. For every index $a \in \mathcal{I}$, we add the rules:

$$\frac{\Delta, F \longrightarrow G}{\Delta, !^a F \longrightarrow G}\ {!^a}_L \qquad \frac{!^{x_1} F_1, \ldots !^{x_n} F_n \longrightarrow G}{!^{x_1} F_1, \ldots !^{x_n} F_n \longrightarrow !^a G}\ {!^a}_R$$

$$\frac{!^{x_1} F_1, \ldots !^{x_n} F_n, F \longrightarrow ?^{x_{n+1}} G}{!^{x_1} F_1, \ldots !^{x_n} F_n, ?^a F \longrightarrow ?^{x_{n+1}} G}\ {?^a}_L \qquad \frac{\Delta \longrightarrow G}{\Delta \longrightarrow ?^a G}\ {?^a}_R$$

where the rules ${!^a}_R$ and ${?^a}_L$ have the side condition that $a \preceq x_i$ for all i. That is, one can only introduce a $!^a$ on the right (or a $?^a$ on the left) if all other formulas in the sequent are marked with indexes that are greater or equal than a.

Finally, for all indexes $a \in \mathcal{U}$, we add the following structural rules:

$$\frac{\Delta, !^a F, !^a F \longrightarrow G}{\Delta, !^a F \longrightarrow G}\ C\ , \quad \frac{\Delta \longrightarrow G}{\Delta, !^a F \longrightarrow G}\ W \quad \text{and} \quad \frac{\Delta \longrightarrow \cdot}{\Delta \longrightarrow ?^a G}\ W$$

That is, we are also free to specify which indexes are unrestricted, namely those appearing in the set $\mathcal{U}$, and which indexes are linear or consumable, namely the remaining indexes.

Danos *et al.* showed in [7] that the classical version of SELL admits cut-elimination. It is also possible to show that the intuitionistic version shown above admits cut-elimination for any signature Σ.

Theorem 2.1: For any signature Σ, the cut-rule is admissible in SELL_Σ.

In the remainder of the paper, we elide the subscript Σ from SELL_Σ, whenever it is clear from the context.

A. Specifying Linear Authorization Logics

This section enters into the details of how one can encode LAL in SELL. Besides containing all the connectives of linear logic, except the exponentials, ! and ?, LAL contains three sorts of families of modalities, namely *says*, *has*, and *knows*, indexed by principal names [13], *e.g.*, $K\, says\, C$, $K\, has\, C$, and $K\, knows\, C$, where K is a principal name and C is a formula. The *says* modality expresses the intent of a principal, while the *has* modality expresses that a principal possesses some consumable resource, which can only be used once, *e.g.*, money, and the *knows* modality expresses the knowledge of a principal, which can be used as many times as needed, *i.e.*, it is an unrestricted resource that can be weakened and contracted.

Intuitively, one can conclude that a principal possesses some resource if one can derive it only from her possessions and from her knowledge base. On the other hand, one can conclude that a principal knows some knowledge if it can be derived only from her knowledge base. Formally, the introduction rules for possession and knowledge modalities are as follows:

$$\frac{\Gamma, F \longrightarrow G}{\Gamma, K\,has\,F \longrightarrow G}\ has_L \qquad \frac{\Psi, \Delta \longrightarrow G}{\Psi, \Delta \longrightarrow K\,has\,G}\ has_R$$

$$\frac{\Gamma, F \longrightarrow G}{\Gamma, K\,knows\,F \longrightarrow G}\ knows_L \qquad \frac{\Psi \longrightarrow G}{\Psi \longrightarrow K\,knows\,G}\ knows_R$$

where Ψ contains only formulas of the form $K\,knows\,C$, while Δ contains only formulas of the form $K\,has\,C$. Moreover, $K\,knows\,F$ can be weakened and contracted on the left.

$$\frac{\Gamma, K\,knows\,F, K\,knows\,F \longrightarrow G}{\Gamma, K\,knows\,F \longrightarrow G}\ C \qquad \frac{\Gamma \longrightarrow G}{\Gamma, K\,knows\,F \longrightarrow G}\ W$$

On the other hand, *says* are families of lax modalities [11], whose introduction rules are as follows:

$$\frac{\Gamma, F \longrightarrow K\,says\,G}{\Gamma, K\,says\,F \longrightarrow K\,says\,G}\ says_L \qquad \frac{\Gamma \longrightarrow G}{\Gamma \longrightarrow K\,says\,G}\ says_R$$

The left inference rule specifies that to prove $K\,says\,G$ one may use the affirmations of the principal K, while the right rule specifies that principals are rational and always affirm formulas that are provable.

Finally, it is assumed that all principals know a common set of global policies Θ. In [13], it was assumed that these rules are in the knowledge base of all principals, *i.e.*, for all formulas $F \in \Theta$ and principal names K, the formula $K\,knows\,F$ appears to the left-hand-side of sequents. Notice that they can be used as many times needed as knowledge is unrestricted.

We start by encoding these modalities in SELL and later in Section II-B we propose extensions that allow one to express a wider range of policies.

Assume given a finite set of principal names $\mathcal{K}$. The set of subexponential indexes is given below:

$I_{\mathcal{K}} = \{h_K, k_K, sL_K, sR_K \mid K \in \mathcal{K}\} \cup \{gl, lin\}$.

Intuitively, h_K is used for specifying *has* modalities, k_K is used for specifying *knows* modalities, sL_K and sR_K are used for specifying *says* modalities, *lin* for linear formulas appearing on the left-hand-side of sequents, and *gl* for the policy rules shared among the principals. Moreover, only the k_K indexes and the index *gl* are unrestricted, that is, $k_K, gl \in \mathcal{U}$, for all $K \in \mathcal{K}$, while the remaining subexponentials are linear. Finally, these indexes are organized in the partial order $\preceq$ as depicted in Figure 1. The subexponential signature specifying this system is denoted by $\Sigma_{\mathcal{K}}$. We will normally use the Greek letter Θ to denote the set of formulas specifying the global policies that are known to all principals.

We encode *says*, *has*, and *knows* modalities using the four types of subexponential indexes above and two encodings $[\![\cdot]\!]_L$ and $[\![\cdot]\!]_R$, for, respectively, negative and positive occurrences of formulas, (or to the left and right-hand-side of the sequent):

$$\begin{array}{lcllcl} [\![K\,has\,C]\!]_L & = & !^{h_K}[\![C]\!]_L & [\![K\,has\,C]\!]_R & = & !^{h_K}[\![C]\!]_R \\ [\![K\,knows\,C]\!]_L & = & !^{k_K}[\![C]\!]_L & [\![K\,knows\,C]\!]_R & = & !^{k_K}[\![C]\!]_R \\ [\![K\,says\,C]\!]_L & = & !^{sL_K}?^{sR_K}[\![C]\!]_L & [\![K\,says\,C]\!]_R & = & ?^{sR_K}[\![C]\!]_R \end{array}$$

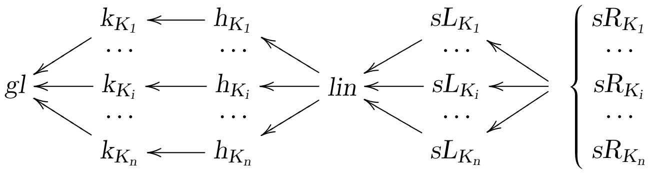

Fig. 1. Graphical representation of the partial order $\preceq$ among subexponential indexes. Here if $a \longrightarrow b$ means that $a \preceq b$. For instance, $h_{K_j} \preceq k_{K_j}$ for all principal names K_j. The bracket denotes that index sR_K is less than sL_K for all principals $K \in \mathcal{K}$, *e.g.*, $sR_{K_1} \preceq sL_{K_n}$. The subexponential signature specifying this system is denoted by $\Sigma_{\mathcal{K}}$, where $\mathcal{K} = \{K_1, \ldots, K_n\}$.

Notice the asymmetry of the encoding of *says* modalities. Its left encoding uses $!^{sL_K}?^{sR_K}$, while the right encoding uses $?^{sR_K}$. As we show below, these encodings capture the requirement for the introduction of a lax modality on the left. For the remaining formulas whose main connective is not a modality, the left-encoding adds an additional $!^{lin}$, while the right-encoding does not do that. For example the encoding of formulas whose main connective is a $\multimap$ is shown below:

$$\begin{array}{lcl} [\![F \multimap G]\!]_L & = & !^{lin}([\![F]\!]_R \multimap [\![G]\!]_L) \\ [\![F \multimap G]\!]_R & = & [\![F]\!]_L \multimap [\![G]\!]_R \end{array}$$

We show in detail some of the the introduction rules of $\text{SELL}_{\Sigma_{\mathcal{K}}}$. In the derivations below, we write $!^a\{F_1, \ldots, F_n\}$ to denote the formulas $!^aF_1, \ldots, !^aF_n$.

Due to the condition on the right introduction of bangs, the right introduction rules for $!^{k_K}$ and $!^{h_K}$ have necessarily the following forms:

$$\frac{!^{gl}\{\Theta\}, !^{k_K}\{\Gamma\} \longrightarrow F}{!^{gl}\{\Theta\}, !^{k_K}\{\Gamma\} \longrightarrow !^{k_K}F} \qquad \frac{!^{gl}\{\Theta\}, !^{k_K}\{\Gamma\}, !^{h_K}\{\Delta\} \longrightarrow F}{!^{gl}\{\Theta\}, !^{k_K}\{\Gamma\}, !^{h_K}\{\Delta\} \longrightarrow !^{h_K}F}$$

As one can easily verify by using the encoding given above and by instatiating Θ as $\emptyset$, the rule to the left corresponds to the right introduction rule for *knows* modalities, as it specifies that one can derive a *knows* formula for a principal K on the right if this formula is derivable using only the knowledge of K. On the other hand, the rule to the right corresponds to the right introduction rule for *has* modalities, as it specifies that one can introduce a *has* formula for the principal K on the right if this formula is derivable only from K's possessions and K's knowledge.

Furthermore, the rules above also illustrate the possibility of distinguishing by using the subexponential *gl* the set of global policies from the private knowledge base of principals. Since they can be contracted and weakened they can be safely be used in LAL proofs. In [13] such global policies were specified by assuming that all principals know these global policies. Both approaches are equivalent as the knowledge of principals is also unrestricted. We use here, however, the former approach, as it explicitly distinguishes the collective global policies which are known to all principals from the private knowledge of principals.

In order to specify the lax restriction for *says* modalities, we use the indexes sL_K and sR_K. Due to the restriction on the left introduction of question-marks, the left introduction rule for $?^{sR_K}$ has the following shape:

$$\frac{\Gamma, F \longrightarrow ?^{sR_K}G}{\Gamma, ?^{sR_K}F \longrightarrow ?^{sR_K}G}$$

where all formulas in Γ are marked with bangs whose indexes belong to the set $\{k_{K_i}, h_{K_i}, sL_{K_i} \mid K_i \in \mathcal{K}\} \cup \{lin, gl\}$. That is, one is only allowed to introduce a $?^{sR_K}$ on the left if the formula to the right hand side of the sequent is marked with $?^{sR_K}$. Furthermore, notice that Γ can contain affirmations of other principals and even formulas that are not part of the knowledge nor possession nor affirmation of any principal. This is the reason why in the encoding above we translate *says* modalities on the left by adding $!^{sL_{K_i}} ?^{sR_{K_i}}$ and formulas whose main connective is not a modality with $!^{lin}$.

We can prove that the encoding above is sound and complete. One needs to take extra care with the $!^{lin}$ used in the encoding. However, since they appear only on the left-hand side of sequents, they do not cause any problems.

Theorem 2.2: A sequent $\Gamma \longrightarrow F$ is provable in the proof system for linear authorization logic shown above if and only if $[\![\Gamma]\!]_L \longrightarrow [\![F]\!]_R$ is provable in SELL.

B. Additional Constructs using SELL

We can use subexponentials to partition policy rules into hierarchies and control their use. Intuitively, higher ranked policies can only be used by principals with higher credentials, such as system administrators, while lower-ranked policies can also be used by other principals with lower credentials. We show how to specify when such policies can and cannot be used in a proof in a simple and *declarative fashion* by using SELL's subexponentials. For simplicity, assume that, besides the set of global policies, there are only two different sets of policy rules a lower-ranked, Γ_L, and a higher-ranked, Γ_H. The general case where there are a greater number of types of policy rules can be specified in a similar fashion.

Formally, we extend the system described in Section II-A with five more indexes:

$I^{LH}_{\mathcal{K}} = I_{\mathcal{K}} \cup \{l, h, e_l, e_h, e_{lh}\}$.

Intuitively, l and h are used to mark formulas specifying the lower and higher-ranked policies as follows $!^{l}\{\Gamma_L\}$ and $!^{h}\{\Gamma_H\}$; the index e_l is used to *disallow* the use of lower-ranked policies; the index e_h is used to *disallow* the use of higher-ranked policies; and the index e_{lh} is used to *disallow* the use of both higher and lower-ranked policies. Since policies can be used in an unrestricted fashion, we assume that l and h are unrestricted indexes, *i.e.*, $l, h \in \mathcal{U}$. The previous partial order relation among the indexes is extended as depicted in Figure 2. The subexponential signature specifying this system is denoted by $\Sigma^{LH}_{\mathcal{K}}$.

The derivation below illustrates, formally, the use of e_l to disallow the use of lower ranked policies in a derivation.

$$\dfrac{\dfrac{\Gamma \longrightarrow F}{\Gamma \longrightarrow !^{e_l} F}\ {!^{e_l}}_R}{\Gamma, !^{l}\{\Gamma_L\} \longrightarrow !^{e_l} F}\ n \times W$$

Notice that according to the preorder depicted in Figure 2, to introduce $!^{e_l}$ on the right one needs to weaken all the formulas marked with $!^{l}$, that is, weaken the lower-ranked policies. Hence, the formula F should be provable without using lower ranked policies. The same reasoning applies to e_h, and e_{lh}, but for, respectively, higher-ranked policies and both higher and lower-ranked policies. The subexponential e_{lh} will also play an important role for our PSPACE-completeness result described in Section V.

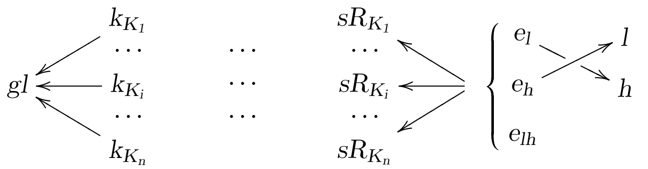

Fig. 2. Graphical representation of the partial order $\leq$ among subexponential indexes. Here if $a \longrightarrow b$ means that $a \leq b$. The bracket denotes that the three indexes e_l, e_h, and e_{lh} are less than sR_K for all principals $K \in \mathcal{K}$, *e.g.*, $e_{lh} \leq sR_{K_1}$. Notice that the indexes l and h are not related to the indexes sR_K, sL_K, h_K nor k_K. The elided part corresponds to the same sub-graph as in Figure 1. The subexponential signature specifying this system is denoted by $\Sigma^{LH}_{\mathcal{K}}$, where $\mathcal{K} = \{K_1, \ldots, K_n\}$.

For a small example using the constructs above, consider the following theory, where we assume all free variables to be universally quantified (including principal names):

$$\begin{array}{l}\text{admin } \mathit{knows}\,(\text{superuser}(K_1)) \otimes K_1\ \mathit{says}\,(K_2\ \mathit{has}\ P) \multimap K_2\ \mathit{has}\ P \\ \text{admin } \mathit{knows}\,(\text{user}(K_1)) \otimes !^{e_h} K_1\ \mathit{says}\,(K_2\ \mathit{has}\ P) \multimap K_2\ \mathit{has}\ P\end{array}$$

The first clause specifies that if the administrator knows that the principal K_1 is a super-user and if K_1 is able to derive from both lower and higher-ranked policies that K_2 has access to P, then K_2 has access to P. On the other hand, the second clause specifies that if administrator knows that K_1 is a normal user, then K_1 may only use the lower ranked policies Γ_L to show that K_2 has access to some resource P. In both cases, however, one can use the global policies Θ.

III. Undecidability

We show that the provability problem for propositional multiplicative fragment of LAL, as described in Section II-A, which is equivalent to the logic described in [13], is *undecidable*. In particular, we encode a two-counter machine [21], which is known to be Turing complete, as a linear authorization theory. Notice that in our encoding we do *not* use the extra expressiveness described in Section II-B.

This result is important in the context of PCA, as it shows that PCA using simple linear authorization policies may be not feasible. Moreover, this undecidability result is also interesting from a proof complexity point of view. It is has been shown that the provability problem for propositional multiplicative additive linear logic with exponentials (MAELL) is undecidable [19]. The same problem, however, for propositional multiplicative linear logic with exponentials (MELL) is still open. In fact, it is believed to be decidable [8]. The difference between MELL and the MELL fragment of LAL is the presence of different modalities, such as *says*, *has*, and *knows*. As we show in our encoding, these modalities play a crucial role for the sound and complete encoding of two-counter Minsky machines, namely for specifying the 0-test instructions. Although we are still not able to make any

(Add r_1) a_k:	$r_1 = r_1 + 1$; goto b_j
(Add r_2) b_k:	$r_2 = r_2 + 1$; goto a_j
(Sub r_1) a_k:	$r_1 = r_1 - 1$; goto b_j
(Sub r_2) b_k:	$r_2 = r_2 - 1$; goto a_j
(0-test r_1) a_k:	if $r_1 = 0$ then goto b_{j_1} else goto b_{j_2}
(0-test r_2) b_k:	if $r_2 = 0$ then goto a_{j_1} else goto a_{j_2}
(Jump$_1$) a_k:	goto b_j
(Jump$_1$) b_k:	goto a_j

Fig. 3. Instructions of a two-counter Minsky machine.

ADD$_1$:	$(A\,has\,r_1 \multimap B\,says\,b_j) \multimap A\,says\,a_k$
ADD$_2$:	$(B\,has\,r_2 \multimap A\,says\,a_j) \multimap B\,says\,b_k$
SUB$_1$:	$(A\,has\,r_1 \otimes B\,says\,b_j) \multimap A\,says\,a_k$
SUB$_2$:	$(B\,has\,r_2 \otimes A\,says\,a_j) \multimap B\,says\,b_k$
0-IF$_1$:	$B\,has\,(B\,says\,b_{j_1}) \multimap A\,says\,a_k$
0-IF$_2$:	$A\,has\,(A\,says\,a_{j_1}) \multimap B\,says\,b_k$
0-ELSE$_1$:	$(A\,has\,r_1 \multimap B\,says\,b_{j_2}) \otimes A\,has\,r_1 \multimap A\,says\,a_k$
0-ELSE$_2$:	$(B\,has\,r_2 \multimap A\,says\,a_{j_2}) \otimes B\,has\,r_2 \multimap B\,says\,b_k$
JUMP$_1$	$B\,says\,b_j \multimap A\,says\,a_k$
JUMP$_2$	$A\,says\,a_j \multimap B\,says\,b_k$
FINAL	$A\,has\,\top \otimes B\,has\,\top \multimap A\,says\,a_0$

Fig. 4. Translation of the instructions of a two-counter Minsky machine M as a set of linear authorization logic formulas Θ_M.

claims about the upper-bound of MELL, it is still interesting that the use of extra modalities leads already to undecidability.

Two-Counter Minsky Machines Let M be a standard two-counter machine containing two registers r_1 and r_2 with natural numbers. Assume that M contains two types of instructions one for a-states and another for b-states. The instructions are depicted in Figure 3. Instructions of M specify its state transition rules. We assume that no instructions are labeled with the same state. The initial state is a_1 and the final state is a_0. Furthermore, a_0 is a halting state so it is distinct from the label of any of M's instructions.

M's configuration is a triple of the form $\langle m, n_1, n_2\rangle$, where m is a state, while n_1 and n_2 are the values of the registers r_1 and r_2. A *computation* performed by M is a sequence of M's configurations such that each step is obtained by applying one of M's instructions: $\langle a_1, n, 0\rangle \xrightarrow{a_1} \cdots \langle a_i, n_i, m_i\rangle \xrightarrow{a_i} \langle b_k, n_k, m_k\rangle \xrightarrow{b_k} \cdots$. A terminating computation is one that ends with a configuration of the form $\langle a_0, n_0, m_0\rangle$ with any values n_0 and m_0 for registers r_1 and r_2.

Encoding Two-Counter Minsky Machines We assume the existence of only two principals A and B. Intuitively, A will be responsible for incrementing and decrementing the register r_1, while B will be responsible for the register r_2.

A machine configuration is encoded as a sequent as follows: The value of the register r_1 is the number of occurrences of $A\,has\,r_1$ formulas in the sequent, while the value of the register r_2 is the number of occurrences of $B\,has\,r_2$ formulas in the sequent. The state of the configuration is encoded as the formula appearing to the right-hand-side of the sequent. If this formula is $A\,says\,a_k$, then the configuration's state is a_k and similarly, if this formula is $B\,says\,b_j$, then the configuration's state is b_j. For example, the following sequent is the translation of the machine M's configuration $\langle a_4, 2, 1\rangle$

$$!^{gl}\{\Theta_M\}, A\,has\,r_1, A\,has\,r_1, B\,has\,r_2 \longrightarrow A\,says\,a_4.$$

Instructions, on the other hand, are translated as the set of global policy rules, Θ_M, depicted in Figure 4.[1] In the derivations below, we will normally elide the $!^{gl}\{\Theta_M\}$ from the sequents, in order to improve presentation. We also assume that they are contracted and weakened whenever needed.

ADD$_i$ is the translation of the instruction Add r_i. Once the clause ADD$_1$ is used, for example, by back-chaining on it, one obtains a derivation with the following shape containing one open premise:

$$\dfrac{\dfrac{}{A\,says\,a_k \longrightarrow A\,says\,a_k}\,I \qquad \dfrac{\Gamma, A\,has\,r_1 \longrightarrow B\,says\,b_j}{\Gamma \longrightarrow A\,has\,r_1 \multimap B\,says\,b_j}\,\multimap_R}{\Gamma \longrightarrow A\,says\,a_k}\,\mathrm{ADD}_1$$

Seeing this derivation from bottom-up, one can verify that it specifies M's Add r_1 instructions. In particular, its end sequent corresponds to the configuration $\langle a_k, m, n\rangle$, while the derivation's open premise corresponds to $\langle b_j, m+1, n\rangle$. The clause SUB$_i$ and JUMP$_i$ follow the same idea, only that SUB$_1$ consumes a has formula, specifying M's Sub instructions, while JUMP$_1$ just changes the formula appearing on the right-hand-side, specifying M's Jump instructions.

The most interesting clauses are the 0-IF$_i$ clauses. In these clauses, we use the modalities explicitly to specify the if case of M's 0-test instructions. In particular, once one back-chains on the clause 0-IF$_1$, due to the restriction on has modalities, the formula $B\,has\,(B\,says\,b_{j_2})$ can only be introduced if there are no $A\,has\,r_1$ formulas in the context. The derivation obtained has therefore the following shape:

$$\dfrac{\dfrac{}{A\,says\,a_k \longrightarrow A\,says\,a_k}\,I \qquad \dfrac{\Gamma \longrightarrow B\,says\,b_{j_1}}{\Gamma \longrightarrow B\,has\,(B\,says\,b_{j_1})}\,has_R}{\Gamma \longrightarrow A\,says\,a_k}\,\text{0-IF}_1$$

with proviso that Γ has no occurrences of $A\,has\,r_1$. Intuitively, this proviso corresponds to the check that $r_1 = 0$. On the other hand, the operational semantics of the else part of the 0-test is captured by using the 0-ELSE$_i$ clauses. In particular, once one back-chains on the clause 0-ELSE$_1$, one obtains a derivation with the following shape, where A_k is the formula $A\,says\,a_k$ and R_1 is the formula $A\,has\,r_1$:

$$\dfrac{\dfrac{}{A_k \longrightarrow A_k}\,I \qquad \dfrac{\dfrac{\Gamma, R_1 \longrightarrow B\,says\,b_j}{\Gamma \longrightarrow R_1 \multimap B\,says\,b_j}\,\multimap_R \qquad \dfrac{}{R_1 \longrightarrow R_1}\,I}{\Gamma, R_1 \longrightarrow (R_1 \multimap B\,says\,b_j) \otimes R_1}\,\otimes_R}{\Gamma, R_1 \longrightarrow A_k}\,\text{0-ELSE}_1$$

Notice that the number of $A\,says\,r_1$ in the open premise is the same as in the end-sequent. However, one can only use this

[1] For better presentation we use the notation with $says, has$, and $knows$ modalities. However, formally these should be interpreted using the left encoding described in Section II-A. For example, the clause ADD$_1$ is in fact $!^{lin}[(!^{h_A}!^{lin}r_1 \multimap ?^{sR_B}b_j) \multimap !^{sL_A}?^{sR_A}!^{lin}a_k]$.

clause if there is at least one $A\,\mathit{says}\,r_1$ in the context of the end-sequent, otherwise the right-most branch is not provable.

Finally, the clause FINAL specifies that one is done once one has reached the final state a_0. By back-chaining on this clause, one obtains the following derivation:

$$\dfrac{\dfrac{}{F \longrightarrow F}\,I \qquad \dfrac{\dfrac{\dfrac{}{\Gamma_A \longrightarrow \top}\,\top_R}{\Gamma_A \longrightarrow A\,\mathit{has}\,\top}\,\mathit{has}_R \quad \dfrac{\dfrac{}{\Gamma_B \longrightarrow \top}\,\top_R}{\Gamma_B \longrightarrow B\,\mathit{has}\,\top}\,\mathit{has}_R}{\Gamma_A, \Gamma_B \longrightarrow A\,\mathit{has}\,\top \otimes B\,\mathit{has}\,\top}\,\otimes_R}{\Gamma_A, \Gamma_B \longrightarrow A\,\mathit{says}\,a_0}\,\text{FINAL}$$

where F is the formula $A\,\mathit{says}\,a_0$ and Γ_A contains only formulas of the form $A\,\mathit{has}\,r_1$, while Γ_B contains only formulas of the form $B\,\mathit{has}\,r_2$. Therefore, any sequent whose right-hand-side is the formula $A\,\mathit{says}\,a_0$ is provable, regardless of how many $A\,\mathit{has}\,r_1$ and $B\,\mathit{has}\,r_2$ appear in the sequent.

From the discussion above, it should be clear that our encoding is complete. Soundness is more complicated. In particular, we need invariants on how *says* formulas may be moved when the context is split. The following two lemmas are enough. The first one states that if two *says* formulas appear on the left-hand-side of a sequent, then the sequent is not provable, while the second lemma states that if a *says* formula appears to the left-hand-side of a sequent that is provable, then there is a computation of M that does not contain any instance of the if case of the 0-test.

Lemma 3.1: Let M be an arbitrary two-counter machine and Γ be an arbitrary multiset of formulas of the form $A\,\mathit{has}\,r_1$ and $B\,\mathit{has}\,r_2$. Let Θ_M be the theory encoding M's instructions. Then for any states q_j, q_i and q_k of M and for any principals $C, D, E \in \{A, B\}$ the sequent $!^{gl}\{\Theta_M\}, C\,\mathit{says}\,q_i, D\,\mathit{says}\,q_j, \Gamma \longrightarrow E\,\mathit{says}\,q_k$ is not provable.

Proof: We proceed by contradiction. Assume that the sequent above is provable and consider its lowest height proof. We cannot apply the initial rule since there are at least two linear formulas, which cannot be weakened, to the left of the sequent, namely, $C\,\mathit{says}\,q_i$ and $D\,\mathit{says}\,q_j$. Hence the only alternative is to use one of the formulas in the theory Θ_M. We can also not use the clause FINAL, since to introduce $A\,\mathit{has}\,\top$ and $B\,\mathit{has}\,\top$ the context must contain only *has* and/or *knows* formulas, which is not the case due to the extra *says* formula. Moreover, one can easily check that at least one premise obtained by using any other clause in Θ_M also has at least two linear formulas of the form *says* formulas in the left-hand-side of the sequent. This contradicts the assumption of that the proof has the lowest height. ■

Lemma 3.2: Let M be an arbitrary two-counter machine M and Γ be a multiset of formulas containing only $A\,\mathit{has}\,r_1$ and $B\,\mathit{has}\,r_2$ formulas with multiplicity of m and n, respectively. Let Θ_M be the theory encoding M's instructions. For any $C, D \in \{A, B\}$ and any states q_j and q_k of M if the sequent $!^{gl}\{\Theta_M\}, D\,\mathit{says}\,q_j, \Gamma \longrightarrow C\,\mathit{says}\,q_k$ is provable, then there is an execution of M from the configuration $\langle q_k, m, n\rangle$ to the configuration $\langle q_j, 0, 0\rangle$, such that the execution does not contain any transition using the if case of a zero test instruction.

Proof: The proof is by induction on the height of the proof of $!^{gl}\{\Theta_M\}, D\,\mathit{says}\,q_j, \Gamma \longrightarrow C\,\mathit{says}\,q_k$. The base case is when the proof ends with an initial rule, in which case $\Gamma = \emptyset$ and $q_k = q_j$. That is, this proof corresponds to the zero length execution.

For the inductive case, one has to consider all possible ways to prove the sequent above. We show only the case for the clause ADD$_1$. The remaining cases follow the same reasoning:

$$\dfrac{A\,\mathit{says}\,a_k, \Gamma' \longrightarrow C\,\mathit{says}\,q_k \qquad \dfrac{D\,\mathit{says}\,q_j, \Gamma'', A\,\mathit{has}\,r_1 \longrightarrow B\,\mathit{says}\,b_j}{D\,\mathit{says}\,q_j, \Gamma'' \longrightarrow A\,\mathit{has}\,r_1 \multimap B\,\mathit{says}\,b_j}}{D\,\mathit{says}\,q_j, \Gamma \longrightarrow C\,\mathit{says}\,q_k}$$

where $\Gamma = \Gamma' \cup \Gamma''$. Notice that from Lemma 3.1, the formula $D\,\mathit{says}\,q_j$ has to be moved to the right branch, otherwise the resulting left premise would contain both $A\,\mathit{says}\,a_k$ and $D\,\mathit{says}\,q_j$ to the left and not be provable. From the inductive hypothesis on the left and right branches, we have that there is an execution from $\langle q_k, m', n'\rangle$ to $\langle a_k, 0, 0\rangle$ and moreover from $\langle b_j, m''+1, n''\rangle$ to $\langle q_j, 0, 0\rangle$, where $m = m' + m''$ and $n = n' + n''$. Since there is no if case of a zero test in any one of these two executions, we can join them as follows:

$$\langle q_k, m' + m'', n' + n''\rangle \longrightarrow \ldots \longrightarrow \langle a_k, m'', n''\rangle \xrightarrow{a_k} \\ \langle b_j, m'' + 1, n''\rangle \longrightarrow \cdots \longrightarrow \langle q_j, 0, 0\rangle.$$

We now show that there is no transition corresponding to the if case of a zero test instruction. As described above, these instructions are specified by the clauses 0-IF$_1$ and 0-IF$_2$. Given Lemma 3.1, the only possible way to use, for instance, the clause 0-IF$_1$ would be as follows:

$$\dfrac{A\,\mathit{says}\,a_k, \Gamma' \longrightarrow C\,\mathit{says}\,q_k \qquad \Gamma'', D\,\mathit{says}\,q_j \longrightarrow B\,\mathit{has}\,(B\,\mathit{says}\,b_{j_1})}{D\,\mathit{says}\,q_j, \Gamma \longrightarrow C\,\mathit{says}\,q_k}$$

where $\Gamma = \Gamma' \cup \Gamma''$ and where the formula $D\,\mathit{says}\,q_j$ moves to the right-branch. However, one cannot introduce $B\,\mathit{has}\,(B\,\mathit{says}\,b_{j_1})$ due to the presence of $D\,\mathit{says}\,q_j$ and therefore the right-premise of this derivation is not provable. ■

With the lemmas above, we can easily show the soundness direction of the following soundness and completeness theorem: (The proof is in the technical report [22].)

Theorem 3.3: Given a two-counter Minsky machine, M, and its translation Θ_M, then there is a terminating computation from $\langle a_1, n, 0\rangle$ if and only if the sequent encoding $\langle a_1, n, 0\rangle$ and the M's instructions, as described above, is provable in SELL$_{\Sigma_{\mathcal{K}}}$, where $\mathcal{K} = \{A, B\}$.

From the encoding above, we can infer that the undecidability of propositional multiplicative fragment of linear authorization logics.

Corollary 3.4: The provability problem for the propositional multiplicative fragment of LAL is undecidable.

IV. Proof Search and MSR

This section paves the way for specifying a fragment of first-order linear authorization logics whose provability problem is PSPACE-complete on the size of the given formula. For this, we use the system introduced in Section II-B, which allows one to express when a formula is provable without using policy rules. This type of operation allows us to formalize a correspondence between the provability problem and the reachability problem for multiset rewrite systems (MSR).

Informally, the state of the system consists of a multiset of facts, specifying the affirmations, possessions, and knowledge of principals, and a state changes by means of rewrite rules that may remove facts from the state, while inserting other facts. However, as in MSR, we would like to determine whether a rule is applicable by using *easy* operations, *e.g.*, checking for membership. In order to capture this intuition, we use the expressiveness gained in Section II-B, namely the ability of specifying when a formula can *only* be derivable without using policy rules.

Firstly, assume that the set of global policies Θ is empty. Moreover, since for simplicity we do not make a distinction between lower-ranked (Γ_L) and higher-ranked policies (Γ_H) in the remainder of this paper, let us assume that all policies are higher-ranked policies (see Section II-B). Consider the following grammar with different types of formulas.

$$\begin{array}{llllll}
T & ::= & \multicolumn{4}{l}{K \; says \; A \mid K \; has \; A \mid K \; says \; T \mid K \; has \; T} \\
Pr & ::= & !^{e_{lh}} T \mid Pr \otimes Pr & Ps & ::= & T \mid Ps \otimes Ps \\
Ps_n & ::= & Ps \mid \exists x. Ps & P & ::= & Pr \multimap Ps_n \mid \forall x. P \\
G & ::= & !^{e_{lh}} T \otimes \top & & &
\end{array}$$

Here, A is an atomic formula. T-formulas are consumable possessions and affirmations of principals. Intuitively, a state of the system consists of a multiset of T-formulas. Notice that T-formulas do not contain $knows$ formulas. As we comment later in this section, adding $knows$ formulas easily leads to the undecidability of the logic.

Policy rules are specified as P-formulas, which are constructed using Pr-formulas (for pre-condition) and Ps_n (for post-condition with nonce creation). According to the grammar above, policy rules have the following shape:

$$\underbrace{\forall \vec{y}.[}_{\text{FV}} \; \underbrace{!^{e_{lh}} T_1 \otimes \cdots \otimes !^{e_{lh}} T_m}_{\text{Pre-condition}} \; \underbrace{\multimap \exists \vec{x}.}_{\text{Nonces}} \; \underbrace{[T_1' \otimes \cdots \otimes T_k']]}_{\text{Post-condition}} \qquad (1)$$

Such a formula can be interpreted as a multiset rewrite rule. The existential variables, $\vec{x}$, appearing in the post-condition specify the creation of nonces, while all free variables (FV) in the pre and post-condition appear in the universally quantified variables $\vec{y}$. Following terminology in proof theory [20], we call this fragment *bipoles*.[2]

The novelty with respect to usual encodings of MSR in linear logic [5], [23] is on the occurrences of $!^{e_{lh}}$ appearing before T-formulas in the pre-condition of P-formulas. As discussed in Section II-B, this connective specifies that one should be able to prove the formulas T_is in the pre-condition without using any policy rules, *i.e.*, the T_is must be derivable only from the T-formulas in the state. The following derivation illustrates the shape of a derivation obtained when using in a proof an instance of a bipole as shown in Equation 1, where fresh values are created accordingly:

$$\begin{array}{c}
T_1'' \longrightarrow T_1 \quad \cdots \quad T_m'' \longrightarrow T_m \qquad !^{h}\{\Gamma_H\}, \mathcal{T}, T_1', \ldots, T_k' \longrightarrow G \\
\hline\hline
!^{h}\{\Gamma_H\}, \mathcal{T}, T_1'', T_2'', \ldots, T_m'' \longrightarrow G
\end{array} \qquad (2)$$

The derivation above can be seen as an inference rule, which from bottom-up behaves like a rewrite rule replacing the T-formulas $T_1'', \ldots, T_m''$ by the T-formulas $T_1', \ldots, T_k'$ appearing at the post-condition of the P-formula used. More importantly, however, all open premises except the right-most have to be proved *without* using any policy rules. This means that the derivations introducing these open premises are simple. In fact, the height of their derivations is bounded by the number of occurrences of modalities in the corresponding open premise (see Lemma 5.1). The paper [13] also points out the importance of such type of derivations in order to prove properties of policies.

G-formulas also deserve some explanation. They are of the form $!^{e_{lh}} T_G \otimes \top$, specifying the goal that one wants to prove (the T-formula T_G) and appearing at the right-hand-side of sequents. As in the pre-condition of P-formulas, the formula $!^{e_{lh}} T_G$ can be intuitively interpreted as checking whether the formula T_G is provable from the state of the system without using policy rules. On the other hand, the formula $\top$ specifies that if T_G is provable, then one is not interested on the remaining formulas ($\mathcal{T}$). Formally, G-formulas are introduced by derivations of the following form:

$$\begin{array}{c}
T'' \longrightarrow T_G \qquad \dfrac{}{!^{h}\{\Gamma_H\}, \mathcal{T} \longrightarrow \top}\; \top_R \\
\hline\hline
!^{h}\{\Gamma_H\}, \mathcal{T}, T'' \longrightarrow !^{e_{lh}} T_G \otimes \top
\end{array} \qquad (3)$$

That is, there is necessarily a T-formula T'' from which one can derive T_G and the right-branch is closed by the introduction of $\top$.

The use of $\top$ is a way of abstracting infinite computations. As argued in [5], [9], distributed systems are endless processes where principals exchange credentials and affirmations forever. Since proofs are finite, we need an abstraction. This is exactly the role that $\top$ is playing. There might be an infinite derivation introducing the right-branch of the derivation above, but by using $\top$, we specify that we are not really interested on it. We are only interested on determining whether the formula T_G can be derived and not on how the remaining credentials are used afterwards.

We can formally show that a sequent is provable if and only if it is provable using derivations of the shapes shown in Derivations 2 and 3. This soundness and completeness result is formally shown by using the soundness and completeness of the *focused discipline* for SELL [23] and the following auxiliary lemma, which is proved by using the fact that T-formulas are linear, that is, they cannot be contracted nor weakened. The proof can be found in the technical report [22].

Lemma 4.1: Let $\Delta \cup \{T\}$ be a multiset of T-formulas. If the sequent $\Delta \longrightarrow T$ is provable in SELL, then Δ has exactly one T-formula, *i.e.*, the sequent has the form $T' \longrightarrow T$.

Theorem 4.2: Let $\mathcal{T}$ be a multiset of T-formulas, Γ_H be a multiset of P-formulas, and G be a G-formula. Let $\mathcal{R}$ be the set

[2] In fact, the class of bipoles is bit more general than the P-formulas above. However, for the lack of a better name and since P-formulas contain most bipoles, we use the same name.

of inference rules obtained from the derivations corresponding to the P-formula in Γ_H (as shown in Derivation 2) and the derivation obtained from the G-formula G (as shown in Derivation 3). Then the sequent $!^h\{\Gamma_H\}, \mathcal{T} \longrightarrow G$ is provable in SELL if and only if it is provable using the rules in $\mathcal{R}$.

Comparison with existing logics In order to illustrate the importance of $!^{e_{lh}}$ for proof search, consider the following clause: $(i)\, A\, says\, a_k \multimap K\, has\, F$, where F is an arbitrary formula which could be written in the logic presented in Section II-A or in [13] and the clauses, Θ_M, in Figure 4 encoding a two-counter Minsky machine. The formula (i) specifies that if the principal A says a_k, then the principal K has the formula F. A derivation introducing (i) has the following shape:

$$\frac{!^h\{\Theta_M\}, \Gamma \longrightarrow A\, says\, a_k \qquad !^h\{\Theta_M\}, \Gamma', K\, has\, F \longrightarrow G}{!^h\{\Theta_M\}, \Gamma, \Gamma' \longrightarrow G}\ (i)$$

As we have shown above, to prove the left-premise of the derivation above is undecidable in general. Therefore, checking whether one can use the clause (i) during proof search is not easy in general. On the other hand, by using $!^{e_{lh}}$ all premises except the right-most in a derivation introducing a P-formula (see Equation 2) can be proved (see Lemma 5.1) since those premises do not contain any P-formulas.

Adding knowledge leads to undecidability From the grammar shown above, one is not allowed to use formulas of the form $K\, knows\, P$. If we allow such formulas, then one can easily show that the provability problem is undecidable.

The proof of undecidability follows from a sound and complete encoding of the Horn implication problem with existentials, which has been shown to be undecidable even without function symbols [10]. In particular, we translate a Horn clause of the form $\forall \vec{y}.[A_1 \wedge \cdots \wedge A_n \supset \exists \vec{x}.A]$, as

$$\forall \vec{y}.[K\, knows\, A_1 \otimes \cdots \otimes K\, knows\, A_n \supset \exists \vec{x}.K\, knows\, A],$$

where $A, A_1, \ldots, A_n$ are atomic formulas and where we use a single principal K. Since $knows$ formulas are unrestricted, one can easily show, by induction on the height of derivations, the soundness and completeness of this translation. That is an atomic formula A is provable from a a Horn theory if and only if the formula $K\, knows\, A$ is provable from its translation. We leave the details to the reader.

Remark: One could refine P-formulas even further. For instance, one could allow formulas in the post-condition of an action to also have bangs marked with some subexponential index, $loc(k)$, denoting the location where some credential is stored. Then by using the same indexes in the bangs of the formulas appearing in the pre-condition, one could enforce that a formula should be only proved using the facts that are in some particular location. For example, the formula $!^{loc(k1)}T \multimap !^{loc(k2)}T'$ specifies that the formula T should be proved using only the formulas in $loc(k1)$ and that the formula T' is to be stored in location $loc(k2)$. This seems to be an interesting application of subexponentials for which leave as future work.

V. PSPACE-completeness

This section shows that the provability problem for a fragment of the system introduced in Section IV is PSPACE-complete. We use most of the machinery used in [16] on the complexity of the reachability problem for MSRs and the machinery introduced in Section IV. In particular, based on a similar notion given in [18], we assume that all policy rules are *balanced*, that is, the number of facts in the pre and post conditions of actions is the same. Formally, in Eq. (1) $m = k$. That is, our policy rules are *balanced bipoles*. This restriction enforces that whenever a policy rule is used during proof search the number of T-formulas in the resulting right-most sequent in Derivation 2 does not change.

As in [18], [17], we assume a finite alphabet, $\mathcal{L}$, with no function symbols. Notice, however, that due to nonce creation, there can be an arbitrary number of symbols in a proof.

PSPACE-hardness It is easy to show that the provability problem for balanced bipoles is PSPACE-hard. We proceed as in [16] by encoding a non-deterministic Turing Machine $\mathcal{M}$ that accepts in space n, by using a single principal K. The details are given in [22].

PSPACE upper bound The PSPACE upper bound is more interesting and is where the machinery introduced in Section II-B pays off. Our PSPACE upper bound is on the following assumptions/inputs:

- $\mathcal{L}$ is finite first-order alphabet without function symbols with J predicate symbols and D constant symbols;
- k is an upper bound on the arity of predicate symbols;
- $\mathcal{P}$ is a finite multiset of balanced bipoles specifying the policy rules;
- $\mathcal{T}$ is a multiset of exactly m T-formulas specifying the initial contents of the sequent. Recall that since all policy rules are balanced bipoles, a policy rule removes and adds the same number of T-formulas from a sequent;
- G is G-formula appearing at the right-hand-side of the sequent.

The problem is to determine whether the sequent $!^h\{\mathcal{P}\}, \mathcal{T} \longrightarrow G$ is provable or not in SELL. Since SELL admits cut-elimination, it is enough to determine whether there is or not a *cut-free* proof introducing the sequent above.

Our PSPACE upper bound is proved by using some of the machinery in [16] and the connections between proof search and MSR execution described in Section IV. However, a main difference to [16] is that here we need to show that it is possible to determine in PSPACE whether one can use a policy rule while searching for a proof. In particular, as illustrated in the Derivation 2 in Section IV, we need to show that one can determine in PSPACE whether a sequent of the form $T_1 \longrightarrow T_2$ is provable or not, where T_1 and T_2 are T-formulas.

We define the size of a T-formula, F, written $|F|$, inductively as follows: $K\, has\, T = K\, says\, T = |T|+1$, and the size of atomic formulas is zero, *i.e.*, $|A| = 0$. The following lemma provides a polynomial bound on the number of steps one needs to take in order to check whether a derivation is a proof the sequent $T_1 \longrightarrow T_2$. The lemma's proof follows from the observation that any (cut-free) derivation introducing the sequent $T_1 \longrightarrow T_2$ does not branch and has its height bounded by $|T_1| + |T_2|$.

Lemma 5.1: Let T_1 and T_2 be two arbitrary T-formulas. The problem of determining whether the sequent $T_1 \longrightarrow T_2$ is provable or not is in NP. In particular, it takes $|T_1| + |T_2|$ steps to check whether an arbitrary cut-free derivation is a proof of the sequent $T_1 \longrightarrow T_2$.

We also show that, while searching for a (cut-free) proof, the size of T-formulas does not grow, *i.e.*, one cannot obtain T-formulas of arbitrary sizes.

Lemma 5.2: Let $\mathcal{S} = !^h\{\mathcal{P}\}, \mathcal{T} \longrightarrow G$ be a sequent, such that the size of any occurrence of a T-formula (including sub-formulas) in $\mathcal{S}$ is bounded by M. Let Ξ be an arbitrary cut-free derivation introducing $\mathcal{S}$. Then the size of all occurrences of T-formulas (including sub-formulas) in Ξ are also bounded by M.

From the parameters above, we obtain M by checking which T-formula appearing anywhere in $\mathcal{P}, \mathcal{T}$ and G, including subformulas, has the greatest size. In typical specifications, such as those given in [13], the value of M is less than 3. Given the lemmas above, we can conclude that the problem of determining whether a policy rule's pre-condition is derivable from some given T-formulas is in PSPACE.

We can now use the machinery given in [16]. First we show the following upper bound on the number of different T-formulas in the system. Notice that following [16], we fix a set with $2mk$ fresh constants to be used as nonces whenever needed. Using the same reasoning as [16], we can show that with this number of constants one can always guarantee the freshness of nonces.

Lemma 5.3: Let $\mathcal{L}$ be a finite alphabet and let M be an upper bound on the size of T-formulas. Then there are at most $MJ(D + 2mk)^k$ different T-formulas in the system, where the parameters are described above.

The following theorem formalizes the PSPACE upper bound for the provability problem when using balanced bipoles.

Theorem 5.4: Given a finite alphabet $\mathcal{L}$, a multiset $\mathcal{P}$ of balanced bipoles, a multiset $\mathcal{T}$ of T-formulas, and a G-formula G, then there is an algorithm that determines whether a sequent $!^h\{\mathcal{P}\}, \mathcal{T} \longrightarrow G$ is provable or not and runs in PSPACE with respect to the following parameters:

1) M is the upper bound on the size of T-formulas;
2) J and D are the number of predicates and constant symbols, respectively, in the alphabet $\mathcal{L}$;
3) m is the number of facts in $\mathcal{T}$;
4) k is an upper bound on the arity of predicate symbols in the alphabet $\mathcal{L}$.

Proof: (Sketch) We use the fact that PSPACE is equal to NPSPACE [24]. Let $i = 0$ and $C_i = \mathcal{T}$ and $G = T_G \otimes \top$. Check whether any formula in $\mathcal{T}$ entails T_G. If so, then output yes. If $i > mMJ(D + 2mk)^k$, then it means that we have encountered the same sequent twice, hence output no. Otherwise, choose non-deterministically a formula P in $\mathcal{P}$ such that its pre-condition is derivable from some formulas $T_1, \ldots, T_n$ in C_i. Construct C_{i+1} from C_i by replacing the T-formulas $T_1, \ldots, T_n$ by the post-condition of P. If necessary chose fresh nonces from the set of $2mk$ constants available. Finally let $i := i + 1$ and repeat.

We show that this algorithm runs in PSPACE. In particular, we can store in PSPACE the set of T-formulas in C_i since it has the same size as the size of $\mathcal{T}$. This is because all formulas in $\mathcal{P}$ are balanced bipoles. Moreover, we can store in PSPACE the value of i in binary as shown below:

$$\begin{aligned}&\log(mMJ(D + 2mk)^k) = \\ &\quad \log(m) + \log(M) + \log(J) + k\log(D + 2mk).\end{aligned}$$

Finally from Lemma 5.1 and 5.2, one can always check in PSPACE whether the pre-condition of a formula in $\mathcal{P}$ is derivable from C_i. Hence the algorithm runs in polynomial space. ■

VI. Example

We show how to specify the student registration similar to the example described in [13] by using balanced bipoles. This example consists of a university registration example, where students may register to courses, which take place at specific timeslots. There are two main principals, a calendar, *cal*, which authorizes free time slots available, and a registrar, *reg*, that controls the entire registration process. We assume the following set of atomic formulas:

- $slot(S, T)$ denoting that the student S is available at time T;
- $cr(S, av/C)$ denoting that the student S has one available credit (av) or that he used a credit to register in the course C.
- $seat(C, av/S)$ denoting that a seat of the course C is available or occupied by the student S.
- $reg(S, C, T)$ denoting the student S is registered at the course C at the time T.
- $course(C, T)$ denoting the course C runs at time slot T.

The goal is to specify this system in such a way that (1) no student registers for more than a stipulated credits, (2) a student does not register for two courses that have the same timeslots, and (3) a maximum registration limit is respected. Here, for simplicity, we assume that each course requires one credit. (It is also possible to specify the general case, but that would require more rules.)

We assume that at the beginning of the semester, the registrar issues an initial number of certificates of the form $reg\,says\,(cr(S, av))$, for each student, and an initial number of certificates of the form $reg\,says\,(seat(C))$ and a unique certificate $reg\,says\,(course(C, T))$ for each course C. Moreover, students get one certificate from the calendar of the form $cal\,says\,(slot(S, T, no))$ for all timeslots T.

The policy specifying this scenario is depicted in Figure 5. It specifies that if the course C at time T has an available seat and the student S has an available credit and is has the timeslot T available, then the student can register causing the seat to be occupied by the student, one of the student's credit to no longer be available and the calender to allocate the timeslot T of the student S as attending the course C.

Notice that since this policy rule behaves as a rewriting rule, it is straightforward to show that the requirements above for this scenario are all satisfied.

$$\forall C, S, T.[!^{e_{lh}} \mathit{reg\,says}\,(\mathit{course}(C, T)) \otimes !^{e_{lh}} \mathit{reg\,says}\,(\mathit{seat}(C, \mathit{av})) \otimes !^{e_{lh}} \mathit{reg\,says}\,(\mathit{cr}(S, \mathit{av})) \otimes !^{e_{lh}} \mathit{cal\,says}\,(\mathit{slot}(S, T))$$
$$\multimap \mathit{reg\,says}\,(\mathit{course}(C, T)) \otimes \mathit{reg\,says}\,(\mathit{seat}(C, S)) \otimes \mathit{reg\,says}\,(\mathit{cr}(S, C)) \otimes \mathit{cal\,says}\,(\mathit{reg}(S, C, T))]$$

Fig. 5. Balanced bipole specifying when a student may register a course.

VII. Conclusions and Related Work

This paper proposed a framework for specifying linear authorization logics that allows one to specify a wider range of policies. We then investigated the complexity of several linear authorization logics including existing logics. We have shown that the provability problem for the propositional multiplicative fragment is undecidable. Then by demonstrating novel connections to multiset rewriting systems, we have also identified a first-order fragment that is PSPACE-complete.

As previously discussed, we improve the work in [13] by proposing a general framework where different linear authorization logics can be specified, which allow for more policies to be specified. For instance, it does not seem possible to specify in the logic proposed in [13] when one is disallowed to use some policies in order to prove a formula. As illustrated by our complexity results, this extra expressiveness seems key to specify tractable fragments for these logics.

Cervesato and Scedrov [5] proposed a framework based on multiset rewriting (MSR) for specifying concurrent processes and also relate their system to linear logic provability. We share some of their concerns, in particular, in conciliating the fact that processes may run forever, while proofs are finite. Our solutions to this problem are similar. While [5] considers open derivations, we close them by using $\top$. [9] applies some of the ideas in [5] to the linear authorization logic proposed in [13]. From our work it seems possible to recover some of the results in [9]. Similarly to our work, [9] also makes use of a focused proof system to reason about policies. We strongly believe that the same reasoning techniques used in [9] can also be apply in our work.

On the complexity of authorization logics, [12] shows that provability problem for propositional classical authorization logics is also PSPACE-complete. On the other hand, there has also been a number of complexity results on linear logic (too many to cite them all here). For instance, [19] investigates the complexity of many fragments of propositional linear logic. In particular, [19] shows that the multiplicative additive fragment with exponentials is undecidable. The unpublished note [6] also shows that the propositional multiplicative fragment of linear logic with subexponentials is undecidable. However, up to our knowledge, this paper contains the first complexity results on linear authorization logics.

This paper also continues the on-going program of investigating MSR systems with balanced actions. In a series of papers [18], [17], [16], we have investigated together with others the complexity for the reachability problem for such MSR systems. This paper capitalized and extends [18], [17], [16] by investigating systems with modalities. For instance, we use the same ideas proposed in [16] to overcome the fact that actions may create fresh values and therefore a proof may contain an unbounded number of symbols. Our PSPACE upper bound algorithm is a conservative extension of the PSPACE upper bound algorithms proposed in [18], [17], [16].

Acknowledgments: We would like to thank Deepak Garg, Cedric Fournet, Max Kanovich, Tajana Ban Kirigin, Hubert Comon-Lundh, Andre Scedrov, and Alwen Tiu for fruitful discussions. Nigam was supported by the Alexander von Humboldt Foundation.

References

[1] M. Abadi. Logic in access control (tutorial notes). In *FOSAD*, 2009.

[2] M. Abadi, M. Burrows, B. W. Lampson, and G. D. Plotkin. A calculus for access control in distributed systems. *ACM Trans. Program. Lang. Syst.*, 15(4):706–734, 1993.

[3] A. W. Appel and E. W. Felten. Proof-carrying authentication. In *CCS*, pages 52–62, 1999.

[4] K. D. Bowers, L. Bauer, D. Garg, F. Pfenning, and M. K. Reiter. Consumable credentials in linear-logic-based access-control systems. In *NDSS*. The Internet Society, 2007.

[5] I. Cervesato and A. Scedrov. Relating state-based and process-based concurrency through linear logic (full-version). *Inf. Comput.*, 207(10):1044–1077, 2009.

[6] K. Chaudhuri. On the expressivity of two refinements of multiplicative exponential linear logic. Unpublished, 2009.

[7] V. Danos, J.-B. Joinet, and H. Schellinx. The structure of exponentials: Uncovering the dynamics of linear logic proofs. In *Kurt Gödel Colloquium*, volume 713, pages 159–171. Springer, 1993.

[8] P. de Groote, B. Guillaume, and S. Salvati. Vector addition tree automata. In *LICS*, pages 64–73. IEEE Computer Society, 2004.

[9] H. DeYoung and F. Pfenning. Reasoning about the consequences of authorization policies in a linear epistemic logic. Workshop on Foundations of Computer Security, Aug. 2009.

[10] N. A. Durgin, P. Lincoln, J. C. Mitchell, and A. Scedrov. Multiset rewriting and the complexity of bounded security protocols. *Journal of Computer Security*, 12(2):247–311, 2004.

[11] M. Fairtlough and M. Mendler. Propositional lax logic. *Inf. Comput.*, 137(1):1–33, 1997.

[12] D. Garg and M. Abadi. A modal deconstruction of access control logics. In *FoSSaCS*, pages 216–230. Springer, 2008.

[13] D. Garg, L. Bauer, K. D. Bowers, F. Pfenning, and M. K. Reiter. A linear logic of authorization and knowledge. In *ESORICS*, pages 297–312. Springer, 2006.

[14] D. Garg and F. Pfenning. Non-interference in constructive authorization logic. In *CSFW*, pages 283–296. IEEE Computer Society, 2006.

[15] J.-Y. Girard. Linear logic. *Theor. Computer Science*, 50:1–102, 1987.

[16] M. Kanovich, T. B. Kirigin, V. Nigam, and A. Scedrov. Bounded memory Dolev-Yao adversaries in collaborative systems. In *FAST*, pages 18–33. Springer, 2010.

[17] M. Kanovich, P. Rowe, and A. Scedrov. Policy compliance in collaborative systems. In *CSF '09*, pages 218–233, 2009.

[18] M. I. Kanovich, P. Rowe, and A. Scedrov. Collaborative planning with confidentiality. *J. Autom. Reasoning*, 46(3-4):389–421, 2011.

[19] P. Lincoln, J. C. Mitchell, A. Scedrov, and N. Shankar. Decision problems for propositional linear logic. In *FOCS*, pages 662–671. 1990.

[20] D. Miller and E. Pimentel. A formal framework for specifying sequent calculus proof systems. Journal submission, July 2011.

[21] M. Minsky. Recursive unsolvability of post's problem of 'tag' and other topics in the theory of turing machines. *Annals of Mathematics*, 1961.

[22] V. Nigam. On the complexity of linear authorization logics. 2012. Available from the author's homepage.

[23] V. Nigam and D. Miller. Algorithmic specifications in linear logic with subexponentials. pages 129–140, 2009.

[24] W. J. Savitch. Relationship between nondeterministic and deterministic tape classes. *Journal of Computer and System Sciences*, 4:177–192, 1970.