Remarks about roles and entitlements

Philippe Balbiani

Remarks about roles and entitlements

Philippe Balbiani *

Toulouse Institute of Computer Science Research
CNRS — Toulouse University, Toulouse, France
philippe.balbiani@irit.fr

Abstract

We introduce an hybrid access control model where abstract pairs consisting of objects and access rights are considered. In this model, an access control matrix is a binary relation of permission between subjects and abstract pairs. Treating sets of subjects as instances of a concept called role and sets of abstract pairs as instances of a concept called entitlement, we introduce in each matrix the binary relations of existential permission and universal permission between roles and entitlements, we analyse their properties, we present the duality between subjects and abstract pairs on one hand and roles and entitlements on the other hand, we extend this duality to the setting with obligations and we demonstrate how this duality is useful by proving the completeness of a propositional modal logic for permissions and obligations.

Résumé

Nous introduisons un modèle hybride de contrôle d'accès dans lequel des paires abstraites constituées d'objets et de droits d'accès sont considérés. Dans ce modèle, une matrice de contrôle d'accès est une relation binaire de permission entre sujets et paires abstraites. Traitant les ensembles de sujets comme les instances d'un concept appelé role et les ensembles de paires abstraites comme les instances d'un concept appelé autorisation, nous introduisons dans chaque matrice les relations binaires de permission existentielle et de permission universelle entre roles et autorisations, nous analysons leurs propriétés, nous présentons la dualité entre sujets et paires abstraites d'une part et roles et autorisations d'autre part, nous étendons cette dualité au modèle avec obligations et nous démontrons comment cette dualité est utile en prouvant la complétude d'une logique modale propositionnelle pour permissions et obligations.

*Address: Toulouse Institute of Computer Science Research, 118 route de Narbonne, 31062 Toulouse Cedex 9, France.

1 Introduction

Accesses of subjects to objects in a computer system are permitted in accordance with a security policy embodied in an access control database. Many computer systems use the access control matrix model to represent security policies [8]. An access control matrix

	o_1	o_2	...
s_1	{r}	$\emptyset$	...
s_2	$\emptyset$	{r, w}	...
s_3	{r, w}	{r, w}	...
s_4	$\emptyset$	{r, w}	...
s_5	{r, w}	{r, w}	...
...	...	...	...

TABLE 1 – Classical form of an access control matrix.

is a relational structure consisting of a nonempty set of subjects (users, processes, etc), a nonempty set of objects (files, tables, etc), access rights (r, w, etc) and a ternary relation between subjects, objects and access rights represented as in Table 1 where subject s_1 has access right r on object o_1, subject s_2 has access rights r and w on object o_2, etc. For computer systems with a lot of subjects and objects, the access control matrices will become very large and most of their entries will be empty. Moreover, many subjects will have the same access rights to the same objects. In order to reduce the cost of security administration for such computer systems, other access control models have been introduced, for instance role-based access control [11] and organization-based access control [1].

Within the context of role-based access control (**RBAC**), it has been proposed that administrators treat sets of subjects as instances of a concept called role. Formally, an **RBAC**-structure consists of a

	o_1	o_2	...
r_a	$\{\mathtt{r}\}$	$\emptyset$	...
r_b	$\emptyset$	$\{\mathtt{r},\mathtt{w}\}$	...
r_c	$\{\mathtt{r},\mathtt{w}\}$	$\{\mathtt{r},\mathtt{w}\}$	...
...	...	...	...

TABLE 2 – A role-based access control matrix.

nonempty set of roles representing sets of subjects, a nonempty set of objects, access rights and a ternary relation between roles, objects and access rights represented as in Table 2 where role r_a has access right $\mathtt{r}$ on object o_1, role r_b has access rights $\mathtt{r}$ and $\mathtt{w}$ on object o_2, etc.

Within the context of organization-based access control (**OrBAC**), sets of subjects are still treated as instances of a concept called role. Moreover, sets of objects are treated as instances of a concept called view and sets of access rights are treated as instances of a concept called activity. Formally, an **OrBAC**-structure consists of a nonempty set of roles representing sets of subjects, a nonempty set of views representing sets of objects, a nonempty set of activities representing sets of access rights, a nonempty set of organizations, a nonempty set of contexts and a 5-ary relation between roles, views, activities, organizations and contexts specifying, given an organization and a context, how permissions — i.e. triples consisting of a role, a view and an activity — are granted.

In this paper, we introduce an hybrid access control model where abstract pairs consisting of objects and access rights are considered. Within its context, sets of subjects are still treated as instances of a concept called role. Moreover, sets of abstract pairs are treated as instances of a concept called entitlement. In our setting, an access control matrix is simply a binary relation of permission between subjects and abstract pairs. In each access control matrix, we introduce the binary relations of existential permission and universal permission between roles and entitlements, we analyse their properties, we show how to build access control matrices from role-entitlement frames satisfying these properties, we present the basic dualities that exist between matrices and frames, we extend these dualities to the setting where obligations are added to permissions and we demonstrate how these dualities are useful by proving the completeness of a propositional modal logic talking about permissions and obligations.

It is not so much the hybrid access control model that we want to develop in this paper as the 2 following ideas : the *duality between matrices and frames* developed in Sections 2–5 and the *propositional modal logic interpreted over matrices and frames* presented in Sections 6–9.

From now on in this paper, for all $n\in\mathbb{N}$, let $(n)=\{i \in \mathbb{N} : \ 1\leq i\leq n\}$ and $[n)=\{i \in \mathbb{N} : \ n<i\}$. The proofs of some of our results can be found in an Appendix.

2 Access control matrices

The accesses of subjects to objects in a computer system can be presented under the form of a matrix where rows represent subjects and columns represent objects. In that case, the entries in a concrete access control matrix specify the access rights that each subject has on each object. The accesses of subjects to objects in a computer system can also be presented under the alternative form of a matrix where rows represent subjects and columns represent abstract pairs consisting of objects and access rights. In that case, the entries in a concrete access control matrix are bits as in Table 3. The above discussion suggests to consider *abstract access control matrices,* i.e. structures of the form (S,Π,P) where S is a nonempty set of *subjects* (with typical members denoted s, t, etc), Π is a nonempty set of *abstract pairs* (with typical members denoted π, ρ, etc) and P is a binary relation of *permission* between subjects and abstract pairs [1].

P	$(o_1,\mathtt{r})$	$(o_1,\mathtt{w})$	$(o_2,\mathtt{r})$	$(o_2,\mathtt{w})$	...
s_1	1	0	0	0	...
s_2	0	0	1	1	...
s_3	1	1	1	1	...
s_4	0	0	1	1	...
s_5	1	1	1	1	...
...	...	...	...	...	...

TABLE 3 – Alternative form of an access control matrix.

Let (S,Π,P) be an abstract access control matrix. For all $s\in S$, let $P(s)=\{\pi\in\Pi : \ sP\pi\}$. For all $\pi\in\Pi$, let $P^{-1}(\pi)=\{s\in S : \ sP\pi\}$. Let $R=\mathcal{P}(S)$ and $E=\mathcal{P}(\Pi)$. Elements of R shall be called *roles* and elements of E shall be called *entitlements.* For all $a\in R$ and for all $\alpha\in E$, we shall say that entitlement α is *existentially permitted to* role a (in symbols $aC_\exists\alpha$) if P intersects $a\times\alpha$, i.e. there exists $s\in a$ and there exists $\pi\in\alpha$ such that $sP\pi$ [2]. For all $a\in R$ and for all $\alpha\in E$, we shall say that entitlement α is *universally permitted to* role a (in symbols $aC_\forall\alpha$) if

1. In some logical models of deontic systems [9], every subject has the permission to perform some action on some object. Since it may be the case in a computer system that a subject has access to no object at all, we do not require in an abstract access control matrix (S,Π,P) that for all $s\in S$, there exists $\pi\in\Pi$ such that $sP\pi$.

2. "Someone in a has the permission to do something in α".

P contains $a \times \alpha$, i.e. for all $s \in a$ and for all $\pi \in \alpha$, $sP\pi$ [3].

Example: If (S, Π, P) is the restriction to $\{s_1, s_2, s_3\}$ and to $\{o_1, o_2\}$ of the abstract access control matrix rep resented in Table 3 then R consists of 8 roles (the subsets of $\{s_1, s_2, s_3\}$) and 16 entitlements (the subsets of $\{(o_1, \mathtt{r}), (o_1, \mathtt{w}), (o_2, \mathtt{r}), (o_2, \mathtt{w})\}$). In particular, entitlement $\{(o_1, \mathtt{r}), (o_1, \mathtt{w})\}$ is existentially permitted to role $\{s_1, s_2\}$ and entitlement $\{(o_2, \mathtt{r}), (o_2, \mathtt{w})\}$ is universally permitted to role $\{s_2, s_3\}$.

It is also of interest to consider the relations $C_{\overrightarrow{\exists\forall}}$, $C_{\overrightarrow{\forall\exists}}$, $C_{\overleftarrow{\exists\forall}}$ and $C_{\overleftarrow{\forall\exists}}$ between roles and entitlements such that for all $a \in R$ and for all $\alpha \in E$,

- $aC_{\overrightarrow{\exists\forall}}\alpha$ if and only if there exists $s \in a$ such that for all $\pi \in \alpha$, $sP\pi$ [4],
- $aC_{\overrightarrow{\forall\exists}}\alpha$ if and only if for all $s \in a$, there exists $\pi \in \alpha$ such that $sP\pi$ [5],
- $aC_{\overleftarrow{\forall\exists}}\alpha$ if and only if there exists $\pi \in \alpha$ such that for all $s \in a$, $sP\pi$ [6],
- $aC_{\overleftarrow{\exists\forall}}\alpha$ if and only if for all $\pi \in \alpha$, there exists $s \in a$ such that $sP\pi$ [7].

We leave the development of the model-theoretic viewpoint about these relations to future investigations.

The properties of existential permissiveness and universal permissiveness are illustrated by the 2 following obvious results.

Lemma 1 *For all $a, b \in R$ and for all $\alpha, \beta \in E$,*

- *if $aC_\exists\alpha$ then $a \neq \emptyset$ and $\alpha \neq \emptyset$,*
- *if $a = \emptyset$ or $\alpha = \emptyset$ then $aC_\forall\alpha$,*
- *$(a \cup b)C_\exists\alpha$ if and only if $aC_\exists\alpha$ or $bC_\exists\alpha$,*
- *$(a \cup b)C_\forall\alpha$ if and only if $aC_\forall\alpha$ and $bC_\forall\alpha$,*
- *$aC_\exists(\alpha \cup \beta)$ if and only if $aC_\exists\alpha$ or $aC_\exists\beta$,*
- *$aC_\forall(\alpha \cup \beta)$ if and only if $aC_\forall\alpha$ and $aC_\forall\beta$.*

Lemma 2 *For all $a \in R$ and for all $\alpha \in E$,*

- *$aC_\exists\alpha$ if and only if there exists $b \in R$ and there exists $\beta \in E$ such that $b \neq \emptyset$, $b \subseteq a$, $\beta \neq \emptyset$, $\beta \subseteq \alpha$ and $bC_\forall\beta$,*
- *$aC_\forall\alpha$ if and only if for all $b \in R$ and for all $\beta \in E$, if $b \neq \emptyset$, $b \subseteq a$, $\beta \neq \emptyset$ and $\beta \subseteq \alpha$ then $bC_\exists\beta$.*

The reader is invited to compare the above properties of existential permissiveness and universal permissiveness to the properties of the contact relations usually considered between regular closed subsets in topological spaces [2, 4, 5, 6] or the properties of the inference relations usually considered between propositions in relational syllogistics [7, 10].

3. "Everyone in a has the permission to do everything in α".
4. "Someone in a has the permission to do everything in α".
5. "Everyone in a has the permission to do something in α".
6. "Something in α is permitted to everyone in a".
7. "Everything in α is permitted to someone in a".

3 Role-entitlement frames

A *role-entitlement frame* is a structure of the form $(R, E, C_\exists, C_\forall)$ where R is a Boolean algebra of *roles* (with typical members denoted a, b, etc), E is a Boolean algebra of *entitlements* (with typical members denoted α, β, etc) and $C_\exists$ and $C_\forall$ are binary relations between roles and entitlements satisfying the properties illustrated in Lemmas 1 and 2.

Let $(R, E, C_\exists, C_\forall)$ be a role-entitlement frame. Obviously,

Lemma 3 *For all atomic roles a and for all atomic entitlements α, $aC_\exists\alpha$ if and only if $aC_\forall\alpha$* [8].

4 Duality matrices/frames

For all abstract access control matrices $\bar{M} = (S, \Pi, P)$, let $\mathtt{f}(\bar{M}) = (R, E, C_\exists, C_\forall)$ where R is the set of all subsets of S, E is the set of all subsets of Π and $C_\exists$ and $C_\forall$ are the binary relations between subsets of S and subsets of Π such that for all $a \in R$ and for all $\alpha \in E$,

- $aC_\exists\alpha$ if and only if there exists $s \in a$ and there exists $\pi \in \alpha$ such that $sP\pi$,
- $aC_\forall\alpha$ if and only if for all $s \in a$ and for all $\pi \in \alpha$, $sP\pi$.

Obviously,

Proposition 1 *For all abstract access control matrices $\bar{M}$, $\mathtt{f}(\bar{M})$ is a role-entitlement frame.*

For all role-entitlement frames $\bar{F} = (R, E, C_\exists, C_\forall)$, let $\mathtt{m}(\bar{F}) = (S, \Pi, P)$ where S is the set of all ultrafilters of R, Π is the set of all ultrafilters of E and P is the binary relation between ultrafilters of R and ultrafilters of E such that for all $s \in S$ and for all $\pi \in \Pi$ [9],

- $sP\pi$ if and only if for all $a \in s$ and for all $\alpha \in \pi$, $aC_\exists\alpha$.

Obviously, for all $s \in S$ and for all $\pi \in \Pi$, $sP\pi$ if and only if there exists $a \in s$ and there exists $\alpha \in \pi$ such that $aC_\forall\alpha$. Moreover,

Proposition 2 *For all role-entitlement frames $\bar{F}$, $\mathtt{m}(\bar{F})$ is an abstract access control matrix.*

The duality between abstract access control matrices and role-entitlement frames is illustrated by the

8. Remind that for all Boolean algebras A and for all $a \in A$, a is *atomic* if $a \neq 0_A$ and for all $b \in A$, if $b \neq 0_A$ and $b \leq_A a$ then $b = a$.

9. Remind that for all Boolean algebras A and for all $U \subseteq A$, U is a *proper filter* if $0_A \notin U$, for all $a, b \in A$, if $a \in U$ and $a \leq_A b$ then $b \in U$ and for all $a, b \in A$, if $a \in U$ and $b \in U$ then $a \cdot_A b \in U$. Moreover, U is an *ultrafilter* if U is a maximal proper filter.

2 following results [10].

Proposition 3 *Let* $\bar{M}=(S,\Pi,P)$ *be an abstract access control matrix,* $\mathtt{f}(\bar{M})=(R',E',C'_\exists,C'_\forall)$ *and* $\mathtt{m}(\mathtt{f}(\bar{M}))=(S'',\Pi'',P'')$. *The function* $h : \bar{M} \longrightarrow \mathtt{m}(\mathtt{f}(\bar{M}))$ *such that for all* $s\in S$, $h(s)=\{a\in R' : s\in a\}$ *and for all* $\pi\in\Pi$, $h(\pi)=\{\alpha\in E' : \pi\in\alpha\}$ *is an isomorphism.*

Proposition 4 *Let* $\bar{F}=(R,E,C_\exists,C_\forall)$ *be a role-entitlement frame,* $\mathtt{m}(\bar{F})=(S',\Pi',P')$ *and* $\mathtt{f}(\mathtt{m}(\bar{F}))=(R'',E'',C''_\exists,C''_\forall)$. *The function* $h : \bar{F} \longrightarrow \mathtt{f}(\mathtt{m}(\bar{F}))$ *such that for all* $a\in R$, $h(a)=\{s\in S' : a\in s\}$ *and for all* $\alpha\in E$, $h(\alpha)=\{\pi\in\Pi' : \alpha\in\pi\}$ *is an embedding.*

5 Introducing obligations

In most logical models of deontic systems [9], if a subject has the obligation to perform an action on some object then it also has the permission to perform that action on that object. An *extended access control matrix* is a structure of the form (S,Π,P,O) where (S,Π,P) is an abstract access control matrix and O is a binary relation of *obligation* between subjects in S and abstract pairs in Π such that for all $s\in S$ and for all $\pi\in\Pi$, if $sO\pi$ then $sP\pi$.

Example: If (S,Π,P) is the abstract access control matrix represented in Table 3 and O is the binary relation between elements of S and elements of Π represented in Table 4 then (S,Π,P,O) is an extended access control matrix.

O	$(o_1,\mathtt{r})$	$(o_1,\mathtt{w})$	$(o_2,\mathtt{r})$	$(o_2,\mathtt{w})$	...
s_1	1	0	0	0	...
s_2	0	0	1	1	...
s_3	0	0	1	1	...
s_4	0	0	1	1	...
s_5	0	0	1	1	...
...	...	...	...	...	...

TABLE 4 – Representation of a binary relation between the subjects and the abstract pairs of the abstract access control matrix represented in Table 3.

Let (S,Π,P,O) be an extended access control matrix. For all $s\in S$, let $O(s)=\{\pi\in\Pi : sO\pi\}$. For all $\pi\in\Pi$, let $O^{-1}(\pi)=\{s\in S : sO\pi\}$. Let $R=\mathcal{P}(S)$ and $E=\mathcal{P}(\Pi)$. For all $a\in R$ and for all $\alpha\in E$, we shall say that α is *existentially obligatory to* a (in symbols $aD_\exists\alpha$) if O intersects $a\times\alpha$, i.e. there exists $s\in a$ and there exists $\pi\in\alpha$ such that $sO\pi$ [11]. For all $a\in R$ and for all $\alpha\in E$, we shall say that α is *universally obligatory to* a (in symbols $aD_\forall\alpha$) if O contains $a\times\alpha$, i.e. for all $s\in a$ and for all $\pi\in\alpha$, $sO\pi$ [12].

Example: If (S,Π,P,O) is the restriction to $\{s_1,s_2,s_3\}$ and $\{o_1,o_2\}$ of the extended abstract access control matrix represented in Tables 3 and 4 then R consists of 8 roles (the subsets of $\{s_1,s_2,s_3\}$) and 16 entitlements (the subsets of $\{(o_1,\mathtt{r}),(o_1,\mathtt{w}),(o_2,\mathtt{r}),(o_2,\mathtt{w})\}$). In particular, entitlement $\{(o_1,\mathtt{r}),(o_1,\mathtt{w})\}$ is existentially obligatory to role $\{s_1,s_2\}$ and entitlement $\{(o_2,\mathtt{r}),(o_2,\mathtt{w})\}$ is universally obligatory to role $\{s_2,s_3\}$.

It is also of interest to consider the relations $D_{\exists\forall}^{\rightarrow}$, $D_{\forall\exists}^{\rightarrow}$, $D_{\exists\forall}^{\leftarrow}$ and $D_{\forall\exists}^{\leftarrow}$ between roles and entitlements such that for all $a\in R$ and for all $\alpha\in E$,

- $aD_{\exists\forall}^{\rightarrow}\alpha$ if and only if there exists $s\in a$ such that for all $\pi\in\alpha$, $sO\pi$ [13],
- $aD_{\forall\exists}^{\rightarrow}\alpha$ if and only if for all $s\in a$, there exists $\pi\in\alpha$ such that $sO\pi$ [14],
- $aD_{\forall\exists}^{\leftarrow}\alpha$ if and only if there exists $\pi\in\alpha$ such that for all $s\in a$, $sO\pi$ [15],
- $aD_{\exists\forall}^{\leftarrow}\alpha$ if and only if for all $\pi\in\alpha$, there exists $s\in a$ such that $sO\pi$ [16].

We leave the development of the model-theoretic viewpoint about these relations to future investigations.

The properties of existential obligation and universal obligation are illustrated by the 3 following obvious results.

Lemma 4 *For all* $a,b\in R$ *and for all* $\alpha,\beta\in E$,

- *if* $aD_\exists\alpha$ *then* $a\neq\emptyset$ *and* $\alpha\neq\emptyset$,
- *if* $a=\emptyset$ *or* $\alpha=\emptyset$ *then* $aD_\forall\alpha$,
- $(a\cup b)D_\exists\alpha$ *if and only if* $aD_\exists\alpha$ *or* $bD_\exists\alpha$,
- $(a\cup b)D_\forall\alpha$ *if and only if* $aD_\forall\alpha$ *and* $bD_\forall\alpha$,
- $aD_\exists(\alpha\cup\beta)$ *if and only if* $aD_\exists\alpha$ *or* $aD_\exists\beta$,
- $aD_\forall(\alpha\cup\beta)$ *if and only if* $aD_\forall\alpha$ *and* $aD_\forall\beta$.

Lemma 5 *For all* $a\in R$ *and for all* $\alpha\in E$,

- $aD_\exists\alpha$ *if and only if there exists* $b\in R$ *and there exists* $\beta\in E$ *such that* $b\neq\emptyset$, $b\subseteq a$, $\beta\neq\emptyset$, $\beta\subseteq\alpha$ *and* $bD_\forall\beta$,
- $aD_\forall\alpha$ *if and only if for all* $b\in R$ *and for all* $\beta\in E$, *if* $b\neq\emptyset$, $b\subseteq a$, $\beta\neq\emptyset$ *and* $\beta\subseteq\alpha$ *then* $bD_\exists\beta$.

10. Remind that for all Boolean algebras A,B and for all functions $f : A \longrightarrow B$, f is a *Boolean homomorphism* if $f(0_A)=0_B$, for all $a\in A$, $f(a^{*A})=f(a)^{*B}$ and for all $a,b\in A$, $f(a+_A b)=f(a)+_B f(b)$. A *Boolean isomorphism* is a bijective Boolean homomorphism. A *Boolean embedding* is an injective Boolean homomorphism.

11. "Someone in a has the obligation to do something in α".
12. "Everyone in a has the obligation to do everything in α".
13. "Someone in a has the obligation to do everything in α".
14. "Everyone in a has the obligation to do something in α".
15. "Something in α is mandatory to everyone in a".
16. "Everything in α is mandatory to someone in a".

Lemma 6 *For all $a \in R$ and for all $\alpha \in E$,*
- *if $aD_\exists\alpha$ then $aC_\exists\alpha$,*
- *if $aD_\forall\alpha$ then $aC_\forall\alpha$.*

An *extended role-entitlement frame* is a structure of the form $(R, E, C_\exists, C_\forall, D_\exists, D_\forall)$ where $(R, E, C_\exists, C_\forall)$ is a role-entitlement frame and $D_\exists$ and $D_\forall$ are binary relations between roles in R and entitlements in E satisfying the properties illustrated in Lemmas 4, 5 and 6.

Let $(R, E, C_\exists, C_\forall, D_\exists, D_\forall)$ be an extended role-entitlement frame. Obviously,

Lemma 7 *For all atomic roles a and for all atomic entitlements α, $aD_\exists\alpha$ if and only if $aD_\forall\alpha$.*

For all extended access control matrices $\bar{M}=(S, \Pi, P, O)$, let $\mathtt{f}(\bar{M})=(R, E, C_\exists, C_\forall, D_\exists, D_\forall)$ where $(R, E, C_\exists, C_\forall)=\mathtt{f}((S, \Pi, P))$ and $D_\exists$ and $D_\forall$ are the binary relations between subsets of S and subsets of Π such that for all $a \in R$ and for all $\alpha \in E$,
- $aD_\exists\alpha$ if and only if there exists $s \in a$ and there exists $\pi \in \alpha$ such that $sO\pi$,
- $aD_\forall\alpha$ if and only if for all $s \in a$ and for all $\pi \in \alpha$, $sO\pi$.

Obviously,

Proposition 5 *For all extended access control matrices $\bar{M}$, $\mathtt{f}(\bar{M})$ is an extended role-entitlement frame.*

For all extended role-entitlement frames $\bar{F}=(R, E, C_\exists, C_\forall, D_\exists, D_\forall)$, let $\mathtt{m}(\bar{F})=(S, \Pi, P, O)$ where $(S, \Pi, P)=\mathtt{m}((R, E, C_\exists, C_\forall))=$ and O is the binary relation between ultrafilters of R and ultrafilters of E such that for all $s \in S$ and for all $\pi \in \Pi$,
- $sO\pi$ if and only if for all $a \in s$ and for all $\alpha \in \pi$, $aD_\exists\alpha$.

Obviously, for all $s \in S$ and for all $\pi \in \Pi$, $sO\pi$ if and only if there exists $a \in s$ and there exists $\alpha \in \pi$ such that $aD_\forall\alpha$. Moreover,

Proposition 6 *For all extended role-entitlement frames $\bar{F}$, $\mathtt{m}(\bar{F})$ is an extended access control matrix.*

The duality between extended access control matrices and extended role-entitlement frames is illustrated by the 2 following results.

Proposition 7 *Let $\bar{M}=(S, \Pi, P, O)$ be an extended access control matrix, $\mathtt{f}(\bar{M})=(R', E', C'_\exists, C'_\forall, D'_\exists, D'_\forall)$ and $\mathtt{m}(\mathtt{f}(\bar{M}))=(S'', \Pi'', P'', O'')$. The function $h : \bar{M} \longrightarrow \mathtt{m}(\mathtt{f}(\bar{M}))$ such that for all $s \in S$, $h(s)=\{a \in R' : s \in a\}$ and for all $\pi \in \Pi$, $h(\pi)=\{\alpha \in E' : \pi \in \alpha\}$ is an isomorphism.*

Proposition 8 *Let $\bar{F}=(R, E, C_\exists, C_\forall, D_\exists, D_\forall)$ be an extended role-entitlement frame, $\mathtt{m}(\bar{F})=(S', \Pi', P', O')$ and $\mathtt{f}(\mathtt{m}(\bar{F}))=(R'', E'', C''_\exists, C''_\forall, D''_\exists, D''_\forall)$. The function $h : \bar{F} \longrightarrow \mathtt{f}(\mathtt{m}(\bar{F}))$ such that for all $a \in R$, $h(a)=\{s \in S' : a \in s\}$ and for all $\alpha \in E$, $h(\alpha)=\{\pi \in \Pi' : \alpha \in \pi\}$ is an embedding.*

6 REL : syntax and semantics

6.1 Syntax

Let **RVAR** be a countable set of *role variables* (with typical members denoted X, Y, etc) and **EVAR** be a countable set of *entitlement variables* (with typical members denoted x, y, etc). Let $(X_1, X_2, \ldots)$ be an enumeration without repetition of **RVAR** and $(x_1, x_2, \ldots)$ be an enumeration without repetition of **EVAR**.

The set **RTER** of all *role terms* (with typical members denoted a, b, etc) is inductively defined as follows :
- $a, b ::= X \mid 0 \mid a^* \mid (a + b)$.

The Boolean constructs 1 and $\cdot$ are defined for role terms by the usual abbreviations : $1 ::= 0^*$ and $(a \cdot b) ::= (a^* + b^*)^*$. The set **ETER** of all *entitlement terms* (with typical members denoted α, β, etc) is inductively defined as follows :
- $\alpha, \beta ::= x \mid 0 \mid \alpha^* \mid (\alpha + \beta)$.

The Boolean constructs 1 and $\cdot$ are defined for entitlement terms by the usual abbreviations : $1 ::= 0^*$ and $(\alpha \cdot \beta) ::= (\alpha^* + \beta^*)^*$.

The set **FOR** of all *formulas* (with typical members denoted φ, ψ, etc) is inductively defined as follows :
- $\varphi, \psi ::= \mathbf{C}_\exists(a, \alpha) \mid \mathbf{C}_\forall(a, \alpha) \mid \mathbf{D}_\exists(a, \alpha) \mid \mathbf{D}_\forall(a, \alpha) \mid a \equiv b \mid \alpha \equiv \beta \mid \bot \mid \neg\varphi \mid (\varphi \vee \psi)$.

We adopt the standard rules for omission of the parenthesis. The Boolean connectives $\top$, $\wedge$, $\rightarrow$ and $\leftrightarrow$ are defined by the usual abbreviations. Let $\mathbf{FOR}_\exists$ be the set of all $\mathbf{C}_\forall$-free $\mathbf{D}_\forall$-free formulas.

Example: Here are examples of formulas :
- $\mathbf{D}_\exists(X, y) \rightarrow \mathbf{C}_\forall(X, y)$,
- $\mathbf{D}_\exists(X_1, y_1) \wedge \mathbf{D}_\forall(X_2, y_2) \rightarrow \mathbf{C}_\forall(X_1 \cdot X_2, y_1 + y_2)$,

the former formula being read "if someone in X has the obligation to do something in y then everyone in X has the permission to do everything in y" and the latter formula being read "if someone in X_1 has the obligation to do something in y_1 and everyone in X_2 has the obligation to do everything in y_2 then everyone in $X_1 \cdot X_2$ has the permission to do everything in $y_1 + y_2$".

On one hand, $\mathbf{C}_\exists$, $\mathbf{C}_\forall$, $\mathbf{D}_\exists$ and $\mathbf{D}_\forall$ can be seen as first-order predicates in a first-order language accepting as arguments pairs consisting of a role term and an entitlement term. On the other hand, $\mathbf{C}_\exists$, $\mathbf{C}_\forall$, $\mathbf{D}_\exists$ and $\mathbf{D}_\forall$ can be seen as diamonds in a propositional

modal language accepting as arguments pairs of Boolean expressions.

6.2 Algebraic semantics

A *valuation* on the extended role-entitlement frame $(R, E, C_\exists, C_\forall, D_\exists, D_\forall)$ is a pair (V, v) consisting of a homomorphism $V : (\mathbf{RTER}, 0, *, +) \longrightarrow R$ and a homomorphism $v : (\mathbf{ETER}, 0, *, +) \longrightarrow E$. *Role-entitlement models* are tuples of the form $(R, E, C_\exists, C_\forall, D_\exists, D_\forall, V, v)$ where $(R, E, C_\exists, C_\forall, D_\exists, D_\forall)$ is an extended role-entitlement frame and (V, v) is a valuation on $(R, E, C_\exists, C_\forall, D_\exists, D_\forall)$.

The Boolean connectives $\bot$, $\neg$ and $\vee$ being interpreted as usual, the unary relation of *satisfiability* of formulas with respect to a role-entitlement model $\mathcal{M}=(R, E, C_\exists, C_\forall, D_\exists, D_\forall, V, v)$ (in symbols $\models_\mathcal{M}$) is inductively defined as follows :

— $\models_\mathcal{M} \mathbf{C}_\exists(a, \alpha)$ if and only if $V(a) C_\exists v(\alpha)$,
— $\models_\mathcal{M} \mathbf{C}_\forall(a, \alpha)$ if and only if $V(a) C_\forall v(\alpha)$,
— $\models_\mathcal{M} \mathbf{D}_\exists(a, \alpha)$ if and only if $V(a) D_\exists v(\alpha)$,
— $\models_\mathcal{M} \mathbf{D}_\forall(a, \alpha)$ if and only if $V(a) D_\forall v(\alpha)$,
— $\models_\mathcal{M} a \equiv b$ if and only if $V(a)=V(b)$,
— $\models_\mathcal{M} \alpha \equiv \beta$ if and only if $v(\alpha)=v(\beta)$.

We shall say that formula φ is *valid* in the extended role-entitlement frame $\bar{F}$ (in symbols $\models_{\bar{F}} \varphi$) if for all role-entitlement models $\mathcal{M}$ based on $\bar{F}$, $\models_\mathcal{M} \varphi$. We shall say that formula φ is *valid* in a class $\mathcal{C}$ of extended role-entitlement frames (in symbols $\models_\mathcal{C} \varphi$) if for all extended role-entitlement frames $\bar{F}$ in $\mathcal{C}$, $\models_{\bar{F}} \varphi$.

6.3 Relational semantics

A *valuation* on the extended access control matrix (S, Π, P, O) is a pair (V, v) consisting of a homomorphism $V : (\mathbf{RTER}, 0, *, +) \longrightarrow \mathcal{P}(S)$ and a homomorphism $v : (\mathbf{ETER}, 0, *, +) \longrightarrow \mathcal{P}(\Pi)$. *Access control models* are tuples of the form (S, Π, P, O, V, v) where (S, Π, P, O) is an extended access control matrix and (V, v) is a valuation on (S, Π, P, O).

The Boolean connectives $\bot$, $\neg$ and $\vee$ being interpreted as usual, the unary relation of *satisfiability* of formulas with respect to an access control model $\mathcal{M}=(S, \Pi, P, O, V, v)$ (in symbols $\models_\mathcal{M}$) is inductively defined as follows :

— $\models_\mathcal{M} \mathbf{C}_\exists(a, \alpha)$ if and only if there exists $s \in V(a)$ and there exists $\pi \in v(\alpha)$ such that $sP\pi$,
— $\models_\mathcal{M} \mathbf{C}_\forall(a, \alpha)$ if and only if for all $s \in V(a)$ and for all $\pi \in v(\alpha)$, $sP\pi$,
— $\models_\mathcal{M} \mathbf{D}_\exists(a, \alpha)$ if and only if there exists $s \in V(a)$ and there exists $\pi \in v(\alpha)$ such that $sO\pi$,
— $\models_\mathcal{M} \mathbf{D}_\forall(a, \alpha)$ if and only if for all $s \in V(a)$ and for all $\pi \in v(\alpha)$, $sO\pi$,
— $\models_\mathcal{M} a \equiv b$ if and only if $V(a)=V(b)$,
— $\models_\mathcal{M} \alpha \equiv \beta$ if and only if $v(\alpha)=v(\beta)$.

We shall say that *formula φ is valid in the extended access control matrix $\bar{M}$* (in symbols $\models_{\bar{M}} \varphi$) if for all access control models $\mathcal{M}$ based on $\bar{M}$, $\models_\mathcal{M} \varphi$. We shall say that *formula φ is valid in a class $\mathcal{C}$ of extended access control matrices* (in symbols $\models_\mathcal{C} \varphi$) if for all extended access control matrices $\bar{M}$ in $\mathcal{C}$, $\models_{\bar{M}} \varphi$.

Example: Let (S, Π, P, O) be the extended abstract access control matrix represented in Tables 3 and 4. If (V, v) is a valuation on it such that $V(X)=\{s_1, s_2\}$ and $v(y)=\{(o_1, \mathtt{r}), (o_1, \mathtt{w})\}$ then $\models_\mathcal{M} \mathbf{D}_\exists(X, y)$ and $\not\models_\mathcal{M} \mathbf{C}_\forall(X, y)$. If (V, v) is a valuation on it such that $V(X_1)=\{s_1, s_2\}$, $V(X_2)=\{s_2, s_3\}$, $v(y_1)=\{(o_1, \mathtt{r}), (o_1, \mathtt{w})\}$ and $v(y_2)=\{(o_2, \mathtt{r}), (o_2, \mathtt{w})\}$ then $\models_\mathcal{M} \mathbf{D}_\exists(X_1, y_1) \wedge \mathbf{D}_\forall(X_2, y_2)$ and $\not\models_\mathcal{M} \mathbf{C}_\forall(X_1 \cdot X_2, y_1 + y_2)$.

7 REL : definability

The 4 following results illustrate the fact that $\mathbf{C}_\exists$, $\mathbf{C}_\forall$, $\mathbf{D}_\exists$ and $\mathbf{D}_\forall$ are not interdefinable when one considers the semantics introduced in Section 6.3. When we prove Proposition 11, they will also illustrate the fact that $\mathbf{C}_\exists$, $\mathbf{C}_\forall$, $\mathbf{D}_\exists$ and $\mathbf{D}_\forall$ are not interdefinable when one considers the semantics introduced in Section 6.2.

Lemma 8 *There exists no $\mathbf{C}_\exists$-free formula φ such that for all extended access control matrices $\bar{M}$, $\models_{\bar{M}} \mathbf{C}_\exists(X, x) \leftrightarrow \varphi$.*

Lemma 9 *There exists no $\mathbf{C}_\forall$-free formula φ such that for all extended access control matrices $\bar{M}$, $\models_{\bar{M}} \mathbf{C}_\forall(X, x) \leftrightarrow \varphi$.*

Lemma 10 *There exists no $\mathbf{D}_\exists$-free formula φ such that for all extended access control matrices $\bar{M}$, $\models_{\bar{M}} \mathbf{D}_\exists(X, x) \leftrightarrow \varphi$.*

Lemma 11 *There exists no $\mathbf{D}_\forall$-free formula φ such that for all extended access control matrices $\bar{M}$, $\models_{\bar{M}} \mathbf{D}_\forall(X, x) \leftrightarrow \varphi$.*

The expressive capacity of the language introduced in Section 6.1 with respect to the semantics introduced in Section 6.3 is illustrated by the 2 following results.

Proposition 9 *For all extended access control matrices $\bar{M}=(S, \Pi, P, O)$,*

— $\models_{\bar{M}} \mathbf{C}_\exists(1, 1)$ *if and only if* $P \neq \emptyset$ [17],
— $\models_{\bar{M}} \neg \mathbf{C}_\forall(1, 1)$ *if and only if* $P \neq S \times \Pi$ [18],

17. "Someone has the permission to do something".
18. "Someone has not the permission to do everything".

— $\models_{\bar{M}} X \not\equiv 0 \to \mathbf{C}_\exists(X,1)$ *if and only if for all* $s\in S$, $P(s)\neq\emptyset$ [19],
— $\models_{\bar{M}} \mathbf{C}_\forall(X,1) \to X \equiv 0$ *if and only if for all* $s\in S$, $P(s)\neq\Pi$ [20],
— $\models_{\bar{M}} x \not\equiv 0 \to \mathbf{C}_\exists(1,x)$ *if and only if for all* $\pi\in\Pi$, $P^{-1}(\pi)\neq\emptyset$ [21],
— $\models_{\bar{M}} \mathbf{C}_\forall(1,x) \to x \equiv 0$ *if and only if for all* $\pi\in\Pi$, $P^{-1}(\pi)\neq S$ [22],
— $\models_{\bar{M}} \mathbf{D}_\exists(1,1)$ *if and only if* $O\neq\emptyset$ [23],
— $\models_{\bar{M}} \neg\mathbf{D}_\forall(1,1)$ *if and only if* $O\neq S\times\Pi$ [24],
— $\models_{\bar{M}} X \not\equiv 0 \to \mathbf{D}_\exists(X,1)$ *if and only if for all* $s\in S$, $O(s)\neq\emptyset$ [25],
— $\models_{\bar{M}} \mathbf{D}_\forall(X,1) \to X \equiv 0$ *if and only if for all* $s\in S$, $O(s)\neq\Pi$ [26],
— $\models_{\bar{M}} x \not\equiv 0 \to \mathbf{D}_\exists(1,x)$ *if and only if for all* $\pi\in\Pi$, $O^{-1}(\pi)\neq\emptyset$ [27],
— $\models_{\bar{M}} \mathbf{D}_\forall(1,x) \to x \equiv 0$ *if and only if for all* $\pi\in\Pi$, $O^{-1}(\pi)\neq S$ [28].

Proposition 10 *For all extended access control matrices* $\bar{M}=(S,\Pi,P,O)$,
— $\models_{\bar{M}} X_1\not\equiv 0 \wedge X_2\not\equiv 0 \to \mathbf{C}_\exists(X_1,x) \vee \mathbf{C}_\exists(X_2,x^*)$ *if and only if for all* $s_1,s_2\in S$, *there exists* $\pi\in\Pi$ *such that* $s_1P\pi$ *and* $s_2P\pi$,
— $\models_{\bar{M}} x_1\not\equiv 0 \wedge x_2\not\equiv 0 \to \mathbf{C}_\exists(X,x_1) \vee \mathbf{C}_\exists(X^*,x_2)$ *if and only if for all* $\pi_1,\pi_2\in\Pi$, *there exists* $s\in S$ *such that* $sP\pi_1$ *and* $sP\pi_2$,
— $\models_{\bar{M}} X_1\not\equiv 0 \wedge X_2\not\equiv 0 \to \mathbf{D}_\exists(X_1,x) \vee \mathbf{D}_\exists(X_2,x^*)$ *if and only if for all* $s_1,s_2\in S$, *there exists* $\pi\in\Pi$ *such that* $s_1O\pi$ *and* $s_2O\pi$,
— $\models_{\bar{M}} x_1\not\equiv 0 \wedge x_2\not\equiv 0 \to \mathbf{D}_\exists(X,x_1) \vee \mathbf{D}_\exists(X^*,x_2)$ *if and only if for all* $\pi_1,\pi_2\in\Pi$, *there exists* $s\in S$ *such that* $sO\pi_1$ *and* $sO\pi_2$.

8 REL : axiomatization

A *logic* is a set $\mathbf{L}$ of formulas such that
(**TAU**) $\mathbf{L}$ contains all tautologies,
— $\mathbf{L}$ contains all formulas of the form
(**A1**) $\mathbf{C}_\exists(a,\alpha) \to a\not\equiv 0 \wedge \alpha\not\equiv 0$,
(**A2**) $a\equiv 0 \vee \alpha\equiv 0 \to \mathbf{C}_\forall(a,\alpha)$,
(**A3**) $\mathbf{C}_\exists(a+b,\alpha) \leftrightarrow \mathbf{C}_\exists(a,\alpha) \vee \mathbf{C}_\exists(b,\alpha)$,
(**A4**) $\mathbf{C}_\forall(a+b,\alpha) \leftrightarrow \mathbf{C}_\forall(a,\alpha) \wedge \mathbf{C}_\forall(b,\alpha)$,
(**A5**) $\mathbf{C}_\exists(a,\alpha+\beta) \leftrightarrow \mathbf{C}_\exists(a,\alpha) \vee \mathbf{C}_\exists(a,\beta)$,
(**A6**) $\mathbf{C}_\forall(a,\alpha+\beta) \leftrightarrow \mathbf{C}_\forall(a,\alpha) \wedge \mathbf{C}_\forall(a,\beta)$,
(**A7**) $a\not\equiv 0 \wedge \alpha\not\equiv 0 \wedge \mathbf{C}_\forall(a,\alpha) \to \mathbf{C}_\exists(a,\alpha)$,
(**A8**) $\mathbf{D}_\exists(a,\alpha) \to a\not\equiv 0 \wedge \alpha\not\equiv 0$,
(**A9**) $a\equiv 0 \vee \alpha\equiv 0 \to \mathbf{D}_\forall(a,\alpha)$,
(**A10**) $\mathbf{D}_\exists(a+b,\alpha) \leftrightarrow \mathbf{D}_\exists(a,\alpha) \vee \mathbf{D}_\exists(b,\alpha)$,
(**A11**) $\mathbf{D}_\forall(a+b,\alpha) \leftrightarrow \mathbf{D}_\forall(a,\alpha) \wedge \mathbf{D}_\forall(b,\alpha)$,
(**A12**) $\mathbf{D}_\exists(a,\alpha+\beta) \leftrightarrow \mathbf{D}_\exists(a,\alpha) \vee \mathbf{D}_\exists(a,\beta)$,
(**A13**) $\mathbf{D}_\forall(a,\alpha+\beta) \leftrightarrow \mathbf{D}_\forall(a,\alpha) \wedge \mathbf{D}_\forall(a,\beta)$,
(**A14**) $a\not\equiv 0 \wedge \alpha\not\equiv 0 \wedge \mathbf{D}_\forall(a,\alpha) \to \mathbf{D}_\exists(a,\alpha)$,
(**A15**) $\mathbf{D}_\exists(a,\alpha) \to \mathbf{C}_\exists(a,\alpha)$,
(**A16**) $\mathbf{D}_\forall(a,\alpha) \to \mathbf{C}_\forall(a,\alpha)$,
(**MP**) $\mathbf{L}$ is closed under modus ponens,
(**US**) $\mathbf{L}$ is closed under uniform substitution,
— $\mathbf{L}$ is closed under all rules of the form
(**R1**) from $X\not\equiv 0 \wedge X\leq a \wedge x\not\equiv 0 \wedge x\leq\alpha \wedge \mathbf{C}_\forall(X,x) \to \varphi$, infer $\mathbf{C}_\exists(a,\alpha) \to \varphi$,
(**R2**∞) from $X\not\equiv 0 \wedge X\leq a \wedge x\not\equiv 0 \wedge x\leq\alpha \wedge \neg\mathbf{C}_\exists(X,x) \to \varphi$, infer $\neg\mathbf{C}_\forall(a,\alpha) \to \varphi$,
(**R3**∞) from $X\not\equiv 0 \wedge X\leq a \wedge x\not\equiv 0 \wedge x\leq\alpha \wedge \mathbf{D}_\forall(X,x) \to \varphi$, infer $\mathbf{D}_\exists(a,\alpha) \to \varphi$,
(**R4**∞) from $X\not\equiv 0 \wedge X\leq a \wedge x\not\equiv 0 \wedge x\leq\alpha \wedge \neg\mathbf{D}_\exists(X,x) \to \varphi$, infer $\neg\mathbf{D}_\forall(a,\alpha) \to \varphi$,
where neither X, nor x occur in a, α or φ.

We write **REL** for the least logic. For all logics $\mathbf{L}$ and for all $\varphi\in\mathbf{FOR}$, we write $\mathbf{L}\oplus\varphi$ for the least logic containing $\mathbf{L}$ and φ. For all logics $\mathbf{L}$ and for all $\Sigma\subseteq\mathbf{FOR}$, we write $\mathbf{L}\oplus\Sigma$ for the least logic containing $\mathbf{L}$ and Σ. For all logics $\mathbf{L}$, an $\mathbf{L}$-*theory* is a set Σ of formulas such that
— Σ contains $\mathbf{L}$,
— Σ is closed under modus ponens,
— Σ is closed under all infinitary rules of the form
(**R1**∞) from $\{X\not\equiv 0 \wedge X\leq a \wedge x\not\equiv 0 \wedge x\leq\alpha \wedge \mathbf{C}_\forall(X,x) \to \varphi : X\in\mathbf{RVAR},\ x\in\mathbf{EVAR}\}$, infer $\mathbf{C}_\exists(a,\alpha) \to \varphi$,
(**R2**∞) from $\{X\not\equiv 0 \wedge X\leq a \wedge x\not\equiv 0 \wedge x\leq\alpha \wedge \neg\mathbf{C}_\exists(X,x) \to \varphi : X\in\mathbf{RVAR},\ x\in\mathbf{EVAR}\}$, infer $\neg\mathbf{C}_\forall(a,\alpha) \to \varphi$,
(**R3**∞) from $\{X\not\equiv 0 \wedge X\leq a \wedge x\not\equiv 0 \wedge x\leq\alpha \wedge \mathbf{D}_\forall(X,x) \to \varphi : X\in\mathbf{RVAR},\ x\in\mathbf{EVAR}\}$, infer $\mathbf{D}_\exists(a,\alpha) \to \varphi$,
(**R4**∞) from $\{X\not\equiv 0 \wedge X\leq a \wedge x\not\equiv 0 \wedge x\leq\alpha \wedge \neg\mathbf{D}_\exists(X,x) \to \varphi : X\in\mathbf{RVAR},\ x\in\mathbf{EVAR}\}$, infer $\neg\mathbf{D}_\forall(a,\alpha) \to \varphi$.

As is well-known, $\mathbf{L}$ is the least $\mathbf{L}$-theory and **FOR** is the greatest $\mathbf{L}$-theory. Obviously, the importance of the infinitary rules (**R1**∞), (**R2**∞), (**R3**∞) and (**R4**∞) is to allow the proof of the following result.

Lemma 12 *Let* $\mathbf{L}$ *be a logic. For all consistent* $\mathbf{L}$-*theories* Σ,
— *for all* $a\in\mathbf{RTER}$ *and for all* $\alpha\in\mathbf{ETER}$, *if* $\mathbf{C}_\exists(a,\alpha)\in\Sigma$ *then there exists* $X\in\mathbf{RVAR}$ *and there exists* $x\in\mathbf{EVAR}$ *such that* $X\not\equiv 0\in\Sigma$, $X\leq a\in\Sigma$, $x\not\equiv 0\in\Sigma$, $x\leq\alpha\in\Sigma$ *and* $\mathbf{C}_\forall(X,x)\in\Sigma$,
— *for all* $a\in\mathbf{RTER}$ *and for all* $\alpha\in\mathbf{ETER}$, *if* $\neg\mathbf{C}_\forall(a,\alpha)\in\Sigma$ *then there exists* $X\in\mathbf{RVAR}$ *and*

19. "Everyone has the permission to do something".
20. "Everyone has not the permission to do everything".
21. "Everything is permitted to someone".
22. "Everything is not permitted to everyone".
23. "Someone has the obligation to do something".
24. "Someone has not the obligation to do everything".
25. "Everyone has the obligation to do something".
26. "Everyone has not the obligation to do everything".
27. "Everything is mandatory to someone".
28. "Everything is not mandatory to everyone".

there exists $x \in \mathbf{EVAR}$ *such that* $X \not\equiv 0 \in \Sigma$, $X \leq a \in \Sigma$, $x \not\equiv 0 \in \Sigma$, $x \leq \alpha \in \Sigma$ *and* $\neg \mathbf{C}_\exists(X,x) \in \Sigma$,
- *for all* $a \in \mathbf{RTER}$ *and for all* $\alpha \in \mathbf{ETER}$, *if* $\mathbf{D}_\exists(a,\alpha) \in \Sigma$ *then there exists* $X \in \mathbf{RVAR}$ *and there exists* $x \in \mathbf{EVAR}$ *such that* $X \not\equiv 0 \in \Sigma$, $X \leq a \in \Sigma$, $x \not\equiv 0 \in \Sigma$, $x \leq \alpha \in \Sigma$ *and* $\mathbf{D}_\forall(X,x) \in \Sigma$,
- *for all* $a \in \mathbf{RTER}$ *and for all* $\alpha \in \mathbf{ETER}$, *if* $\neg \mathbf{D}_\forall(a,\alpha) \in \Sigma$ *then there exists* $X \in \mathbf{RVAR}$ *and there exists* $x \in \mathbf{EVAR}$ *such that* $X \not\equiv 0 \in \Sigma$, $X \leq a \in \Sigma$, $x \not\equiv 0 \in \Sigma$, $x \leq \alpha \in \Sigma$ *and* $\neg \mathbf{D}_\exists(X,x) \in \Sigma$.

For all logics $\mathbf{L}$, the $\mathbf{L}$-theory Σ is *consistent* if $\bot \notin \Sigma$. As is well-known, an $\mathbf{L}$-theory Σ is consistent if and only if $\Sigma \neq \mathbf{FOR}$. For all logics $\mathbf{L}$, for all $\mathbf{L}$-theories Σ and for all formula φ, let $\Sigma + \varphi = \{\psi \in \mathbf{FOR} : \varphi \rightarrow \psi \in \Sigma\}$. As is well-known,

Lemma 13 *For all logics* $\mathbf{L}$, *for all* $\mathbf{L}$*-theories* Σ *and for all formula* φ, $\Sigma + \varphi$ *is an* $\mathbf{L}$*-theory. Moreover,* $\Sigma + \varphi$ *is consistent if and only if* $\neg\varphi \notin \Sigma$.

The main instrument in proofs of completeness is the so-called Lindenbaum Lemma. Its proof is standard and can be found in many papers or textbooks [29].

Lemma 14 (Lindenbaum Lemma) *Let* $\mathbf{L}$ *be a logic. For all consistent* $\mathbf{L}$*-theories* Σ, *there exists a maximal consistent* $\mathbf{L}$*-theory* Δ *such that* $\Sigma \subseteq \Delta$.

The next result states the completeness of **REL** with respect to validity in the class of all extended role-entitlement frames and with respect to validity in the class of all extended access control matrices.

Proposition 11 *For all* $\varphi \in \mathbf{FOR}$, *the following conditions are equivalent :*

1. $\varphi \in \mathbf{REL}$,
2. φ *is valid in the class of all extended role-entitlement frames,*
3. φ *is valid in the class of all extended access control matrices.*

The next result states the completeness of some extensions of **REL** with respect to validity in restricted classes of extended access control matrices.

Proposition 12 *For all* $\varphi \in \mathbf{FOR}$,
- $\varphi \in \mathbf{REL} \oplus \mathbf{C}_\exists(1,1)$ *if and only if* φ *is valid in the class of all extended access control matrices* (S,Π,P,O) *such that* $P \neq \emptyset$,
- $\varphi \in \mathbf{REL} \oplus \neg\mathbf{C}_\forall(1,1)$ *if and only if* φ *is valid in the class of all extended access control matrices* (S,Π,P,O) *such that* $P \neq S \times \Pi$,
- $\varphi \in \mathbf{REL} \oplus X \not\equiv 0 \rightarrow \mathbf{C}_\exists(X,1)$ *if and only if* φ *is valid in the class of all extended access control matrices* (S,Π,P,O) *such that for all* $s \in S$, $P(s) \neq \emptyset$,
- $\varphi \in \mathbf{REL} \oplus \mathbf{C}_\forall(X,1) \rightarrow X \equiv 0$ *if and only if* φ *is valid in the class of all extended access control matrices* (S,Π,P,O) *such that for all* $s \in S$, $P(s) \neq \Pi$,
- $\varphi \in \mathbf{REL} \oplus x \not\equiv 0 \rightarrow \mathbf{C}_\exists(1,x)$ *if and only if* φ *is valid in the class of all extended access control matrices* (S,Π,P,O) *such that for all* $\pi \in \Pi$, $P^{-1}(\pi) \neq \emptyset$,
- $\varphi \in \mathbf{REL} \oplus \mathbf{C}_\forall(1,x) \rightarrow x \equiv 0$ *if and only if* φ *is valid in the class of all extended access control matrices* (S,Π,P,O) *such that for all* $\pi \in \Pi$, $P^{-1}(\pi) \neq S$,
- $\varphi \in \mathbf{REL} \oplus \mathbf{D}_\exists(1,1)$ *if and only if* φ *is valid in the class of all extended access control matrices* (S,Π,P,O) *such that* $O \neq \emptyset$,
- $\varphi \in \mathbf{REL} \oplus \neg\mathbf{D}_\forall(1,1)$ *if and only if* φ *is valid in the class of all extended access control matrices* (S,Π,P,O) *such that* $O \neq S \times \Pi$,
- $\varphi \in \mathbf{REL} \oplus X \not\equiv 0 \rightarrow \mathbf{D}_\exists(X,1)$ *if and only if* φ *is valid in the class of all extended access control matrices* (S,Π,P,O) *such that for all* $s \in S$, $O(s) \neq \emptyset$,
- $\varphi \in \mathbf{REL} \oplus \mathbf{D}_\forall(X,1) \rightarrow X \equiv 0$ *if and only if* φ *is valid in the class of all extended access control matrices* (S,Π,P,O) *such that for all* $s \in S$, $O(s) \neq \Pi$,
- $\varphi \in \mathbf{REL} \oplus x \not\equiv 0 \rightarrow \mathbf{D}_\exists(1,x)$ *if and only if* φ *is valid in the class of all extended access control matrices* (S,Π,P,O) *such that for all* $\pi \in \Pi$, $O^{-1}(\pi) \neq \emptyset$,
- $\varphi \in \mathbf{REL} \oplus \mathbf{D}_\forall(1,x) \rightarrow x \equiv 0$ *if and only if* φ *is valid in the class of all extended access control matrices* (S,Π,P,O) *such that for all* $\pi \in \Pi$, $O^{-1}(\pi) \neq S$.

9 REL : decidability

Let $\mathbf{DER}_\exists$ be the decision problem defined as follows :

input : $\varphi, \psi \in \mathbf{FOR}_\exists$,

output : determine whether $\psi \in \mathbf{REL} \oplus \varphi$.

The following result will be crucial for the proof of the decidability of $\mathbf{DER}_\exists$.

Proposition 13 *For all* $\varphi, \psi \in \mathbf{FOR}_\exists$, *the following conditions are equivalent :*

1. $\psi \in \mathbf{REL} \oplus \varphi$,
2. ψ *is valid in the class of all finite extended access control matrices validating* φ,

29. For example, see [2, Lemma 3.2].

3. *ψ is valid in the class of all extended access control matrices validating φ.*

Now, we are in a position to prove the main result of this section.

Proposition 14 $\mathbf{DER}_\exists$ *is decidable.*

Let **DER** be the decision problem defined as follows :

input : $\varphi, \psi \in \mathbf{FOR}$,

output : determine whether $\psi \in \mathbf{REL} \oplus \varphi$.

It is still unknown whether **DER** is decidable.

10 Conclusion

In this paper, the propositional modal logic **REL** for permissions and obligations has been introduced together with some of its extensions. Interpreted over extended role-entitlement frames or extended access control matrices, it constitutes a decidable setting for reasoning about the access rights of subjects in computer systems.

An axiomatization of **REL** has been proposed and its completeness has been proved. The decision problem of derivability has been presented in the case of $\mathbf{C}_\forall$-free $\mathbf{D}_\forall$-free formulas and its decidability has been proved. The decidability of the decision problem of derivability in the general case where the connectives $\mathbf{C}_\forall$ and $\mathbf{D}_\forall$ are allowed is still unknown.

It is not so much the hybrid access control model that we want to develop in this paper as the 2 following ideas : the *duality between matrices and frames* developed in Sections 2–5 and the *propositional modal logic interpreted over matrices and frames* presented in Sections 6–9. We believe our reasoning can be adapted to other categories of relational structures.

Acknowledgements

Special acknowledgement is heartily granted to our colleagues of the Toulouse Institute of Computer Science Research (Toulouse, France) for many stimulating discussions about the subject of this paper. We also make a point of strongly thanking the referees for their feedback : their useful suggestions have been essential for improving the correctness and the readability of a preliminary version of this paper.

Références

[1] Abou El Kalam, A., R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miège, C. Saurel, and G. Troessin, 'Organization based access control', In : *Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks,* IEEE (2003) 120–131.

[2] Balbiani, P., T. Tinchev, and D. Vakarelov, 'Modal logics for region-based theories of space', *Fundamenta Informaticæ* **81** (2007) 29–82.

[3] Davey, B., and H. Priestley, *Introduction to Lattices and Order. Second Edition,* Cambridge University Press (2002).

[4] Dimov, G., and D. Vakarelov, 'Contact algebras and region-based theory of space : a proximity approach — I', *Fundamenta Informaticæ* **74** (2006) 209–249.

[5] Dimov, G., and D. Vakarelov, 'Contact algebras and region-based theory of space : proximity approach — II', *Fundamenta Informaticæ* **74** (2006) 251–282.

[6] Düntsch, I., and D. Vakarelov, 'Region-based theory of discrete spaces : a proximity approach', *Annals of Mathematics and Artificial Intelligence* **49** (2007) 5–14.

[7] Ivanov, N., and D. Vakarelov, 'A system of relational syllogistic including full Boolean reasoning', *Journal of Logic, Language and Information* **21** (2012) 433–459.

[8] Lampson, B., 'Protection', *Operating Systems Review* **8** (1974) 18–24.

[9] Parent, X., and L. van der Torre, *Introduction to Deontic Logic and Normative Systems,* College Publications (2018).

[10] Pratt-Hartmann, I., and L. Moss, 'Logics for the relational syllogistic', *The Review of Symbolic Logic* **2** (2009) 647–683.

[11] Sandhu, R., E. Coyne, H. Feinstein, and C. Youman, 'Role-based access control models', *IEEE Computer* **29** (1996) 38–47.

[12] Wechler, W., *Universal Algebra for Computer Scientists,* Springer (1992).

Appendix

Proof of Proposition 3 : The proof of the fact that the function h is a Boolean isomorphism is left to the reader.

Let $s \in S$ and $\pi \in \Pi$. We demonstrate $sP\pi$ if and only if $h(s)P''h(\pi)$.

Suppose $sP\pi$. Hence, $\{s\}C'_\forall\{\pi\}$. Since $\{s\} \in h(s)$ and $\{\pi\} \in h(\pi)$, $h(s)P''h(\pi)$.

Reciprocally, suppose $h(s)P''h(\pi)$. Let $a{\in}h(s)$ and $\alpha{\in}h(\pi)$ be such that $aC'_\forall\alpha$. Thus, $s{\in}a$ and $\pi{\in}\alpha$. Since $aC'_\forall\alpha$, $sP\pi$.

Proof of Proposition 4 : The proof of the fact that the function h is a Boolean embedding is well-known [3, Theorem 10.22].

Let $a{\in}R$ and $\alpha{\in}E$. We demonstrate $aC_\exists\alpha$ if and only if $h(a)C''_\exists h(\alpha)$.

Suppose $aC_\exists\alpha$. Let $s_0{=}\{b{\in}R : a{\leq_R}b\}$ and $\pi_0{=}\{\beta{\in}E : \alpha{\leq_E}\beta\}$. Obviously, s_0 is a filter of R such that $a{\in}s_0$ and π_0 is a filter of E such that $\alpha{\in}\pi_0$. Moreover, since $aC_\exists\alpha$, for all $b{\in}s_0$ and for all $\beta{\in}\pi_0$, $bC_\exists\beta$. Let $\mathbf{H}{=}\{(s,\pi) : s$ is a filter of R and π is a filter of E such that $a{\in}s$, $\alpha{\in}\pi$ and for all $b{\in}s$ and for all $\beta{\in}\pi$, $bC_\exists\beta\}$. Since s_0 is a filter of R such that $a{\in}s_0$, π_0 is a filter of E such that $\alpha{\in}\pi_0$ and for all $b{\in}s_0$ and for all $\beta{\in}\pi_0$, $bC_\exists\beta$, $\mathbf{H}$ is a nonempty set. Let $\ll$ be the partial order on $\mathbf{H}$ such that for all $(s,\pi),(s',\pi'){\in}\mathbf{H}$, $(s,\pi){\ll}(s',\pi')$ if and only if $s{\subseteq}s'$ and $\pi{\subseteq}\pi'$. Obviously, every chain in $(\mathbf{H},\ll)$ has an upper bound. By Zorn's Lemma [12, Page 35], let (s,π) be a maximal element in $(\mathbf{H},\ll)$. The proof of the fact that s is an ultrafilter of R and π is an ultrafilter of E is left to the reader. Since $a{\in}s$ and $\alpha{\in}\pi$, $s{\in}h(a)$ and $\pi{\in}h(\alpha)$. Since for all $b{\in}s$ and for all $\beta{\in}\pi$, $bC_\exists\beta$, $sP'\pi$. Since $s{\in}h(a)$ and $\pi{\in}h(\alpha)$, $h(a)C''_\exists h(\alpha)$.

Reciprocally, suppose $h(a)C''_\exists h(\alpha)$. Let $s{\in}h(a)$ and $\pi{\in}h(\alpha)$ be such that $sP'\pi$. Hence, $a{\in}s$ and $\alpha{\in}\pi$. Since $sP'\pi$, let $b{\in}s$ and $\beta{\in}\pi$ be such that $bC_\forall\beta$. Thus, $(a{\cdot}b)C_\forall(\alpha{\cdot}\beta)$. Since $a{\in}s$, $\alpha{\in}\pi$, $b{\in}s$ and $\beta{\in}\pi$, $a{\cdot}b{\neq}0_R$ and $\alpha{\cdot}\beta{\neq}0_E$. Since $(a{\cdot}b)C_\forall(\alpha{\cdot}\beta)$, $(a{\cdot}b)C_\exists(\alpha{\cdot}\beta)$. Consequently, $aC_\exists\alpha$.

Let $a{\in}R$ and $\alpha{\in}E$. We demonstrate $aC_\forall\alpha$ if and only if $h(a)C''_\forall h(\alpha)$.

Suppose not $h(a)C''_\forall h(\alpha)$. Let $s{\in}h(a)$ and $\pi{\in}h(\alpha)$ be such that not $sP'\pi$. Hence, $a{\in}s$ and $\alpha{\in}\pi$. Since not $sP'\pi$, not $aC_\forall\alpha$.

Reciprocally, suppose not $aC_\forall\alpha$. Let $b{\in}R$ and $\beta{\in}E$ be such that $b{\neq}0_R$, $b{\leq_R}a$, $\beta{\neq}0_E$, $\beta{\leq_E}\alpha$ and not $bC_\exists\beta$. Thus, $h(b){\neq}0_{R''}$, $h(b){\leq_{R''}}h(a)$, $h(\beta){\neq}0_{E''}$, $h(\beta){\leq_{E''}}h(\alpha)$ and not $h(b)C''_\exists h(\beta)$. Consequently, not $h(a)C''_\forall h(\alpha)$.

Proof of Proposition 7 : Similar to the proof of Proposition 3.

Proof of Proposition 8 : Similar to the proof of Proposition 4.

Proof of Lemma 8 : For the sake of the contradiction, suppose φ is a $\mathbf{C}_\exists$-free formula such that for all extended access control matrices $\bar{M}$, $\models_{\bar{M}} \mathbf{C}_\exists(X,x) \leftrightarrow \varphi$. Without loss of generality, we can assume that X is the only role variable occurring in φ and x is the only entitlement variable occurring in φ. Let (S,Π,P,O) be the extended access control matrix such that $S{=}\{0,1,2,3,4\}$, $\Pi{=}\{0,1,2,3,4\}$, $P{=}\{(0,0),(1,1),(2,2)\}$ and $O{=}\emptyset$. Since for all extended access control matrices $\bar{M}$, $\models_{\bar{M}} \mathbf{C}_\exists(X,x) \leftrightarrow \varphi$, $\models_{(S,\Pi,P,O)} \mathbf{C}_\exists(X,x) \leftrightarrow \varphi$. Let $\mathcal{M}{=}(S,\Pi,P,O,V,v)$ and $\mathcal{M}'{=}(S,\Pi,P,O,V',v')$ be access control models based on (S,Π,P,O) and such that $V(X){=}\{2,3,4\}$, $v(x){=}\{2,3,4\}$, $V'(X){=}\{3,4\}$ and $v'(x){=}\{3,4\}$. Since $\models_{(S,\Pi,P,O)} \mathbf{C}_\exists(X,x) \leftrightarrow \varphi$, $\models_{\mathcal{M}} \mathbf{C}_\exists(X,x) \leftrightarrow \varphi$ and $\models_{\mathcal{M}'} \mathbf{C}_\exists(X,x) \leftrightarrow \varphi$. Obviously, $\models_{\mathcal{M}} \mathbf{C}_\exists(X,x)$ and $\not\models_{\mathcal{M}'} \mathbf{C}_\exists(X,x)$. Since $\models_{\mathcal{M}} \mathbf{C}_\exists(X,x) \leftrightarrow \varphi$ and $\models_{\mathcal{M}'} \mathbf{C}_\exists(X,x) \leftrightarrow \varphi$, $\models_{\mathcal{M}} \varphi$ and $\not\models_{\mathcal{M}'} \varphi$. As the reader may easily verify by induction on the $\mathbf{C}_\exists$-free formula ψ, if X is the only role variable occurring in ψ and x is the only entitlement variable occurring in ψ then $\models_{\mathcal{M}} \psi$ if and only if $\models_{\mathcal{M}'} \psi$. Since φ is a $\mathbf{C}_\exists$-free formula such that X is the only role variable occurring in φ, x is the only entitlement variable occurring in φ and $\models_{\mathcal{M}} \varphi$, $\models_{\mathcal{M}'} \varphi$: a contradiction.

Proof of Lemma 9 : For the sake of the contradiction, suppose φ is a $\mathbf{C}_\forall$-free formula such that for all extended access control matrices $\bar{M}$, $\models_{\bar{M}} \mathbf{C}_\forall(X,x) \leftrightarrow \varphi$. Without loss of generality, we can assume that X is the only role variable occurring in φ and x is the only entitlement variable occurring in φ. Let (S,Π,P,O) be the extended access control matrix such that $S{=}\{0,1,2,3,4\}$, $\Pi{=}\{0,1,2,3,4\}$, $P{=}\{(0,0),(1,1),(2,2)\}$ and $O{=}\emptyset$. Since for all extended access control matrices $\bar{M}$, $\models_{\bar{M}} \mathbf{C}_\forall(X,x) \leftrightarrow \varphi$, $\models_{(S,\Pi,P,O)} \mathbf{C}_\forall(X,x) \leftrightarrow \varphi$. Let $\mathcal{M}{=}(S,\Pi,P,O,V,v)$ and $\mathcal{M}'{=}(S,\Pi,P,O,V',v')$ be access control models based on (S,Π,P,O) and such that $V(X){=}\{0\}$, $v(x){=}\{0\}$, $V'(X){=}\{0,1\}$ and $v'(x){=}\{0,1\}$. Since $\models_{(S,\Pi,P,O)} \mathbf{C}_\forall(X,x) \leftrightarrow \varphi$, $\models_{\mathcal{M}} \mathbf{C}_\forall(X,x) \leftrightarrow \varphi$ and $\models_{\mathcal{M}'} \mathbf{C}_\forall(X,x) \leftrightarrow \varphi$. Obviously, $\models_{\mathcal{M}} \mathbf{C}_\forall(X,x)$ and $\not\models_{\mathcal{M}'} \mathbf{C}_\forall(X,x)$. Since $\models_{\mathcal{M}} \mathbf{C}_\forall(X,x) \leftrightarrow \varphi$ and $\models_{\mathcal{M}'} \mathbf{C}_\forall(X,x) \leftrightarrow \varphi$, $\models_{\mathcal{M}} \varphi$ and $\not\models_{\mathcal{M}'} \varphi$. As the reader may easily verify by induction on the $\mathbf{C}_\forall$-free formula ψ, if X is the only role variable occurring in ψ and x is the only entitlement variable occurring in ψ then $\models_{\mathcal{M}} \psi$ if and only if $\models_{\mathcal{M}'} \psi$. Since φ is a $\mathbf{C}_\forall$-free formula such that X is the only role variable occurring in φ, x is the only entitlement variable

occurring in φ and $\models_{\mathcal{M}} \varphi$, $\models_{\mathcal{M}'} \varphi$: a contradiction.

Proof of Lemma 10 : Similar to the proof of Lemma 8.

Proof of Lemma 11 : Similar to the proof of Lemma 9.

Proof of Proposition 9 : Let $\bar{M}=(S,\Pi,P,O)$ be an extended access control matrix.

We only demonstrate the item $\models_{\bar{M}}\ \mathbf{C}_{\exists}(1,1)$ if and only if $P\neq\emptyset$, leaving to the reader the proof of the other items.

Suppose $\models_{\bar{M}}\ \mathbf{C}_{\exists}(1,1)$. Let $\mathcal{M}=(\bar{M},V,v)$ be an access control model based on $\bar{M}$. Since $\models_{\bar{M}} \mathbf{C}_{\exists}(1,1)$, $\models_{\mathcal{M}} \mathbf{C}_{\exists}(1,1)$. Let $s\in V(1)$ and $\pi\in v(1)$ be such that $sP\pi$. Hence, $P\neq\emptyset$.

Suppose $P\neq\emptyset$. Let $s\in S$ and $\pi\in\Pi$ be such that $sP\pi$. Let $\mathcal{M}=(\bar{M},V,v)$ be an arbitrary access control model based on $\bar{M}$. Since $sP\pi$, $s\in V(1)$ and $\pi\in v(1)$, $\models_{\mathcal{M}} \mathbf{C}_{\exists}(1,1)$. Since $\mathcal{M}$ is an arbitrary access control model based on $\bar{M}$, $\models_{\bar{M}} \mathbf{C}_{\exists}(1,1)$.

Proof of Proposition 10 : Let $\bar{M}=(S,\Pi,P,O)$ be an extended access control matrix.

We only demonstrate the item $\models_{\bar{M}} X_1\neq 0 \wedge X_2\neq 0 \rightarrow \mathbf{C}_{\exists}(X_1,x)\vee\mathbf{C}_{\exists}(X_2,x^*)$ if and only if for all $s_1,s_2\in S$, there exists $\pi\in\Pi$ such that $s_1P\pi$ and $s_2P\pi$, leaving to the reader the proof of the other items.

Suppose $\models_{\bar{M}} X_1\neq 0\wedge X_2\neq 0 \rightarrow \mathbf{C}_{\exists}(X_1,x)\vee\mathbf{C}_{\exists}(X_2,x^*)$. For the sake of the contradiction, suppose there exists $s_1,s_2\in S$ such that for all $\pi\in\Pi$, not $s_1P\pi$, or not $s_2P\pi$. Let (V,v) be a valuation on $\bar{M}$ such that $V(X_1)=\{s_1\}$, $V(X_2)=\{s_2\}$ and $v(x)=P(s_2)$. Obviously, $\models_{(\bar{M},(V,v))}\ X_1\neq 0 \wedge X_2\neq 0$. Moreover, since $V(X_2)=\{s_2\}$ and $v(x)=P(s_2)$, $\not\models_{(\bar{M},(V,v))} \mathbf{C}_{\exists}(X_2,x^*)$. Since $\models_{\bar{M}} X_1\neq 0 \wedge X_2\neq 0 \rightarrow \mathbf{C}_{\exists}(X_1,x)\vee\mathbf{C}_{\exists}(X_2,x^*)$, $\models_{(\bar{M},(V,v))}\ \mathbf{C}_{\exists}(X_1,x)$. Since $V(X_1)=\{s_1\}$ and $v(x)=P(s_2)$, there exists $\pi\in\Pi$ such that $s_1P\pi$, or $s_2P\pi$: a contradiction.

Suppose for all $s_1,s_2\in S$, there exists $\pi\in\Pi$ such that $s_1P\pi$ and $s_2P\pi$. For the sake of the contradiction, suppose $\not\models_{\bar{M}} X_1\neq 0\wedge X_2\neq 0 \rightarrow \mathbf{C}_{\exists}(X_1,x)\vee\mathbf{C}_{\exists}(X_2,x^*)$. Let (V,v) be a valuation on $\bar{M}$ such that $\models_{(\bar{M},(V,v))}\ X_1\neq 0 \wedge X_2\neq 0$, $\not\models_{(\bar{M},(V,v))}\ \mathbf{C}_{\exists}(X_1,x)$ and $\not\models_{(\bar{M},(V,v))}\ \mathbf{C}_{\exists}(X_2,x^*)$. Let $t_1,t_2\in S$ be such that $t_1\in V(X_1)$ and $t_2\in V(X_2)$. Since for all $s_1,s_2\in S$, there exists $\pi\in\Pi$ such that $s_1P\pi$ and $s_2P\pi$, let $\pi\in\Pi$ such that $t_1P\pi$ and $t_2P\pi$. Obviously, $\pi\in v(x)$, or $\pi\in v(x^*)$. In the former case, since $t_1\in V(X_1)$ and $s_1P\pi$, $\models_{(\bar{M},(V,v))}\ \mathbf{C}_{\exists}(X_1,x)$: a contradiction. In the latter case, since $t_2\in V(X_2)$ and $s_2P\pi$, $\models_{(\bar{M},(V,v))} \mathbf{C}_{\exists}(X_2,x^*)$: a contradiction.

Proof of Proposition 11 : Let $\varphi\in$**FOR**.

(**1** $\Rightarrow$ **2**) Suppose $\varphi\in$**REL**. Hence, there is a proof of φ from the formulas (**TAU**) and (**A1**)–(**A16**) and the rules (**MP**), (**US**) and (**R1**)–(**R4**). The proof of the fact that the formulas (**TAU**) and (**A1**)–(**A16**) are valid in the class of all extended role-entitlement frames and the rules (**MP**), (**US**) and (**R1**)–(**R4**) preserve validity in the class of all extended role-entitlement frames is left to the reader. Thus, by induction on the length of the proof of φ, φ is valid in the class of all extended role-entitlement frames.

(**2** $\Rightarrow$ **3**) Suppose φ is not valid in the class of all extended access control matrices. Let $\bar{M}=(S,\Pi,P,O)$ be an extended access control matrix such that $\not\models_{\bar{M}}\ \varphi$. Let $\mathcal{M}=(\bar{M},V,v)$ be an access control model based on $\bar{M}$ and such that $\not\models_{\mathcal{M}}\ \varphi$. Let $\mathtt{f}(\bar{M})=(R,E,C_{\exists},C_{\forall},D_{\exists},D_{\forall})$. Let $\mathcal{M}'=(R,E,C_{\exists},C_{\forall},D_{\exists},D_{\forall},V,v)$. As the reader may easily verify by induction on the formula ψ, $\models_{\mathcal{M}}\ \psi$ iff $\models_{\mathcal{M}'}\ \psi$. Since $\not\models_{\mathcal{M}}\ \varphi$, $\not\models_{\mathcal{M}'}\ \varphi$. Consequently, $\not\models_{\mathtt{f}(\bar{M})}\ \varphi$. Hence, φ is not valid in the class of all extended role-entitlement frames.

(**3** $\Rightarrow$ **1**) Suppose $\varphi\notin$**REL**. Thus, by Lemma 13, the **REL**-theory **REL** $+\ \neg\varphi$ is consistent. Consequently, by Lemma 14, let Σ be a maximal **REL**-consistent theory such that $\neg\varphi\in\Sigma$. Hence, $\varphi\notin\Sigma$. Let $\asymp_{\Sigma}$ be the equivalence relation on **RTER** and $\bowtie_{\Sigma}$ be the equivalence relation on **ETER** such that for all $a,b\in$**RTER** and for all $\alpha,\beta\in$**ETER**,

- $a\asymp_{\Sigma} b$ if and only if $a\equiv b\in\Sigma$,
- $\alpha\bowtie_{\Sigma}\beta$ if and only if $\alpha\equiv\beta\in\Sigma$.

The *equivalence class modulo* $\asymp_{\Sigma}$ *with* $a\in$**RTER** *as its representative* is written $[a]_{\Sigma}$ and the *equivalence class modulo* $\bowtie_{\Sigma}$ *with* $\alpha\in$**ETER** *as its representative* is written $[\alpha]_{\Sigma}$. The proof of the fact that **RTER**$/\asymp_{\Sigma}$ — the quotient set of **RTER** modulo $\asymp_{\Sigma}$ — and **ETER**$/\bowtie_{\Sigma}$ — the quotient set of **ETER** modulo $\bowtie_{\Sigma}$ — are Boolean algebras is left to the reader. Let $\bar{M}_{\Sigma}=(S_{\Sigma},\Pi_{\Sigma},P_{\Sigma},O_{\Sigma})$ be the structure defined as follows :

- S_{Σ} is the set of all ultrafilters in **RTER**$/\asymp_{\Sigma}$,
- Π_{Σ} is the set of all ultrafilters in **ETER**$/\bowtie_{\Sigma}$,
- P_{Σ} is the binary relation between S_{Σ} and Π_{Σ} such that for all $s\in S_{\Sigma}$ and for all $\pi\in\Pi_{\Sigma}$, $sP_{\Sigma}\pi$

if and only if for all $a \in \mathbf{RTER}$ and for all $\alpha \in \mathbf{ETER}$, if $a \in s$ and $\alpha \in \pi$ then $\mathbf{C}_\exists(a,\alpha) \in \Sigma$,
— O_Σ is the binary relation between S_Σ and Π_Σ such that for all $s \in S_\Sigma$ and for all $\pi \in \Pi_\Sigma$, $sP_\Sigma\pi$ if and only if for all $a \in \mathbf{RTER}$ and for all $\alpha \in \mathbf{ETER}$, if $a \in s$ and $\alpha \in \pi$ then $\mathbf{D}_\exists(a,\alpha) \in \Sigma$.

Obviously, $\bar{M}_\Sigma$ is an extended access control matrix. Let (V_Σ, v_Σ) be the valuation on $\bar{M}_\Sigma$ such that for all $X \in \mathbf{RVAR}$ and for all $x \in \mathbf{EVAR}$,

— $V_\Sigma(X) = \{s \in S_\Sigma : X \in s\}$,
— $v_\Sigma(x) = \{\pi \in \Pi_\Sigma : x \in \pi\}$.

Let $\mathcal{M}_\Sigma = (\bar{M}_\Sigma, V_\Sigma, v_\Sigma)$ — the *canonical model determined by* Σ. As the reader may easily verify by induction on the formula ψ, $\models_{\mathcal{M}_\Sigma} \psi$ if and only if $\psi \in \Sigma$. Since $\varphi \notin \Sigma$, $\not\models_{\mathcal{M}_\Sigma} \varphi$. Thus, φ is not valid in the class of all extended access control matrices.

Proof of Proposition 12 : Let $\varphi \in \mathbf{FOR}$.

We only demonstrate the item $\varphi \in \mathbf{REL} \oplus \mathbf{C}_\exists(1,1)$ if and only if φ is valid in the class of all extended access control matrices (S, Π, P, O) such that $P \neq \emptyset$, leaving to the reader the proof of the other items.

Suppose $\varphi \in \mathbf{REL} \oplus \mathbf{C}_\exists(1,1)$. Hence, there is a proof of φ from the formulas (**TAU**), (**A1**)–(**A16**) and $\mathbf{C}_\exists(1,1)$ and the rules (**MP**), (**US**) and (**R1**)–(**R4**). The proof of the fact that the formulas (**TAU**) and (**A1**)–(**A16**) are valid in the class of all extended access control matrices (S, Π, P, O) such that $P \neq \emptyset$ and the rules (**MP**), (**US**) and (**R1**)–(**R4**) preserve validity in the class of all extended access control matrices (S, Π, P, O) such that $P \neq \emptyset$ is left to the reader. By Proposition 9, the formula $\mathbf{C}_\exists(1,1)$ is valid in the class of all extended access control matrices (S, Π, P, O) such that $P \neq \emptyset$. Thus, by induction on the length of the proof of φ, φ is valid in the class of all extended access control matrices (S, Π, P, O) such that $P \neq \emptyset$.

Suppose $\varphi \notin \mathbf{REL} \oplus \mathbf{C}_\exists(1,1)$. Consequently, the $(\mathbf{REL} \oplus \mathbf{C}_\exists(1,1))$-theory $(\mathbf{REL} \oplus \mathbf{C}_\exists(1,1)) + \neg\varphi$ is consistent. Hence, by Lemma 14, let Σ be a maximal $(\mathbf{REL} \oplus \mathbf{C}_\exists(1,1))$-consistent theory such that $\neg\varphi \in \Sigma$. Leaving to the reader the proof that the extended access control matrix $(S_\Sigma, \Pi_\Sigma, P_\Sigma, O_\Sigma)$ defined from Σ as in the proof of Proposition 11 is such that $P_\Sigma \neq \emptyset$, we conclude that φ is not valid in the class of all extended access control matrices (S, Π, P, O) such that $P \neq \emptyset$.

Proof of Proposition 13 : Let $\varphi \in \mathbf{FOR}_\exists$.

(**1** $\Rightarrow$ **2**) Suppose $\psi \in \mathbf{REL} \oplus \varphi$. Hence, there is a proof of ψ from the formulas (**TAU**), (**A1**), (**A3**), (**A5**), (**A8**), (**A10**), (**A12**), (**A15**) and φ and the rules (**MP**) and (**US**). The proof of the fact that the formulas (**TAU**), (**A1**), (**A3**), (**A5**), (**A8**), (**A10**), (**A12**) and (**A15**) are valid in the class of all finite extended access control matrices validating φ and the rules (**MP**) and (**US**) preserve validity in the class of all finite extended access control matrices validating φ is left to the reader. Thus, by induction on the length of the proof of ψ, ψ is valid in the class of all finite extended access control matrices validating φ.

(**2** $\Rightarrow$ **3**) Suppose ψ is valid in the class of all finite extended access control matrices validating φ. For the sake of the contradiction, suppose ψ is not valid in the class of all extended access control matrices validating φ. Let $\bar{M} = (S, \Pi, P, O)$ be an extended access control matrix validating φ and such that $\not\models_{\bar{M}} \psi$. Let $\mathcal{M} = (\bar{M}, V, v)$ be an access control model based on $\bar{M}$ and such that $\not\models_{\mathcal{M}} \psi$. Let $\approx_f$ be the equivalence relation on S such that for all $s, s' \in S$, $s \approx_f s'$ if and only if for all role variables X occurring in φ or ψ, $s \in V(X)$ if and only if $s' \in V(X)$ and $\doteq_f$ be the equivalence relation on Π such that for all $\pi, \pi' \in \Pi$, $\pi \doteq_f \pi'$ if and only if for all entitlement variables x occurring in φ or ψ, $\pi \in v(x)$ if and only if $\pi' \in v(x)$. The *equivalence class modulo* $\approx_f$ *with* $s \in S$ *as its representative* is written $[s]_f$ and the *equivalence class modulo* $\doteq_f$ *with* $\pi \in \Pi$ *as its representative* is written $[\pi]_f$. Obviously, there exists only finitely many equivalence classes modulo $\approx_f$ and there exists only finitely many equivalence classes modulo $\doteq_f$. Let $\bar{M}_f = (S_f, \Pi_f, P_f, O_f)$ be the structure defined as follows :

— S_f is $S/\approx_f$ — the quotient set of S modulo $\approx_f$,
— Π_f is $\Pi/\doteq_f$ — the quotient set of Π modulo $\doteq_f$,
— P_f is the binary relation between S_f and Π_f such that for all $s \in S$ and for all $\pi \in \Pi$, $[s]_f P_f [\pi]_f$ if and only if there exists $s' \in S$ and there exists $\pi' \in \Pi$ such that $s \approx_f s'$, $\pi \doteq_f \pi'$ and $s' P \pi'$,
— O_ψ is the binary relation between S_f and Π_f such that for all $s \in S$ and for all $\pi \in \Pi$, $[s]_f O_f [\pi]_f$ if and only if there exists $s' \in S$ and there exists $\pi' \in \Pi$ such that $s \approx_f s'$, $\pi \doteq_f \pi'$ and $s' O \pi'$.

Obviously, $\bar{M}_f$ is a finite extended access control matrix. Let (V_f, v_f) be a valuation on $\bar{M}_\psi$ such that for all role variables X occurring in φ or ψ and for all entitlement variables x occurring in φ or ψ,

— $V_f(X) = \{[s]_f \in S_f : s \in V(X)\}$,
— $v_f(x) = \{[\pi]_f \in \Pi_f : \pi \in v(x)\}$.

Let $\mathcal{M}_f = (\bar{M}_f, V_f, v_f)$ — the *filtration of* $\mathcal{M}$ *determined by* φ *and* ψ. As the reader may easily verify by induction on the formula χ sharing the same variables as φ and ψ, $\models_{\mathcal{M}_f} \chi$ if and only if $\models_{\mathcal{M}} \chi$. Since

$\not\models_{\mathcal{M}} \psi$, $\not\models_{\mathcal{M}_f} \psi$. Consequently, $\not\models_{\bar{M}_f} \psi$. Since ψ is valid in the class of all finite extended access control matrices validating φ, $\bar{M}_f$ does not validate φ. Let $\mathcal{M}'=(\bar{M}_f, V', v')$ be an access control model based on $\bar{M}_f$ and such that $\not\models_{\mathcal{M}'} \varphi$. Let $\mathcal{M}''=(\bar{M}, V'', v'')$ be an access control model based on $\bar{M}$ such that for all role variables X occurring in φ or ψ and for all entitlement variables x occurring in φ or ψ,

— $V''(X)=\bigcup\{\bigcap\{V(a) : \ a$ is a role term sharing the same variables as φ and ψ and such that $[s]_f \in V_f(a)\} : \ [s]_f \in V'(X)\}$,

— $v''(x)=\bigcup\{\bigcap\{v(\alpha) : \ \alpha$ is an entitlement term sharing the same variables as φ and ψ and such that $[\pi]_f \in v_f(\alpha)\} : \ [\pi]_f \in v'(x)\}$.

As the reader may easily verify by induction on the formula χ sharing the same variables as φ and ψ, $\models_{\mathcal{M}''} \chi$ if and only if $\models_{\mathcal{M}'} \chi$. Since $\not\models_{\mathcal{M}'} \varphi$, $\not\models_{\mathcal{M}''} \varphi$. Hence, $\not\models_{\bar{M}} \varphi$. Thus, $\bar{M}$ does not validate φ : a contradiction.

(**3** $\Rightarrow$ **1**) Suppose $\psi \notin \mathbf{REL} \oplus \varphi$. Consequently, by Lemma 13, the $(\mathbf{REL} \oplus \varphi)$-theory $(\mathbf{REL} \oplus \varphi) + \neg\psi$ is consistent. Consequently, by Lemma 14, let Σ be a maximal $(\mathbf{REL} \oplus \varphi)$-consistent theory such that $\neg\psi \in \Sigma$. Hence, $\psi \notin \Sigma$. Let $\mathcal{M}_\Sigma=(\bar{M}_\Sigma, V_\Sigma, v_\Sigma)$ be the canonical model determined by Σ. As demonstrated in the proof of Proposition 11, since $\psi \notin \Sigma$, $\not\models_{\mathcal{M}_\Sigma} \psi$. Let $\mathcal{M}_f=(\bar{M}_f, V_f, v_f)$ be the filtration of $\mathcal{M}_\Sigma$ determined by φ and ψ. As demonstrated above, since $\not\models_{\mathcal{M}_\Sigma} \psi$, $\not\models_{\mathcal{M}_f} \psi$. Moreover, $\bar{M}_f$ validates φ.

Proof of Proposition 14 : By Proposition 13 and the fact that

— given a finite extended access control matrix $\bar{M}$ and $\varphi \in \mathbf{FOR}_\exists$, one can easily determine whether $\models_{\bar{M}} \varphi$,

— given a finite extended access control matrix $\bar{M}$ and $\psi \in \mathbf{FOR}_\exists$, one can easily determine whether there exists an access control model $\mathcal{M}$ based on $\bar{M}$ and such that $\models_{\mathcal{M}} \psi$.