UNIVERSITY OF OSLO
Department of Informatics

Deontic Modalities over Synchronous Actions – technicalities [1]

Research Report No. 381

Cristian Prisacariu

Isbn 82-7368-341-9
Issn 0806-3036

December 2008

Deontic Modalities over Synchronous Actions – technicalities [†]

Cristian Prisacariu[‡]

December 2008

Abstract

The work reported here steams from the need of a more practical interpretation of the deontic logic. We follow the recent ought-to-do approach where the deontic modalities are applied over actions instead of over expressions. This allows an easy integration with the propositional dynamic logic or the modal μ-calculus; and from here a whole set of tools e.g. for model checking or for runtime monitoring can now be easily adapted to the deontic modalities. We consider the regular actions enriched with the synchrony operator to model synchronous execution of actions. The interpretation that we give to the logic is biased by the natural properties which the deontic modalities are required to respect when used in the legal environment. Technically the paper presents a semantics based on an algebraic formalism for the actions and on normative structures for the deontic modalities. One source of difficulty comes from the synchrony operator over actions. The properties of the deontic modalities are presented as validities or nonvalidities. The logic enjoys the tree model property and the finite model property and decidability follows from this.

[†]Partially supported by the Nordunet3 project "COSoDIS – Contract-Oriented Software Development for Internet Services" (`http://www.ifi.uio.no/cosodis/`).

[‡]Dept. of Informatics – Univ. of Oslo, P.O. Box 1080 Blindern, N-0316 Oslo, Norway. E-mail: cristi@ifi.uio.no

Contents

1 Introduction

Standard deontic logic (SDL) considers the deontic modalities (obligation O, permission P, and prohibition F) applied over expressions of the logic [McN06]; this is known as the *ought-to-be* approach. When looking at the axiomatization of SDL it is a modal logic where the axioms K (distributivity) and D (seriality or unboundedness) hold and the *necessity rule* is taken besides the MP. On the other hand the axiom T (reflexivity) does not hold in SDL.[1] In a model theoretic view O behaves as the modal *necessity* and $O(p)$ has the meaning that it is true iff *p is true in all permissible worlds*. In this setting the reachability relation on the models of modal logic is called (and viewed as) a *permissibility relation*. To have an intuition about the deontic motivation behind the axoms of SDL consider the seriality axiom D. This axiom is required because of the need to capture the fact that it is not possible to have both $O(p)$ and $F(p)$ in the same state. $F(p)$ is the abreviation for $O(\neg p)$.[2] If no transition exists from the current state then both $O(p)$ and $O(\neg p)$ are trivially true. Therefore it is required for at least one transition from each state where $O(p)$ holds.

The standard deontic logic is notorious for its philosophical problems. It was advocated by G.H. von Wright [VW68] that deontic logic would benefit from a foundation of actions, i.e. a logic of actions, and many of the philosophical paradoxes of SDL would go away. Work in this direction was done by K. Segerberg for introducing the actions inside the deontic modalities [Seg82]. In computer science it is now well established that dynamic logic [Pra76, FL77] is the logic of actions and the deontic logic community is adopting it in various forms as e.g. in the seminal work of J.-J.Ch. Meyer [Mey88] or in the new approach of [BWM01] based on modal μ-calculus (which subsumes propositional dynamic logic). For a history of the developments of the logic of actions see the survey [Seg92].

In this paper we follow this complementary approach to *ought-to-be* which is *ought-to-do* that applies deontic modalities over actions. Compared to the related works [Mey88, BWM01, vdM96, CM] the investigation presented in this paper is different in several ways:

1. The deontic modalities are not encoded in the dynamic logic of actions but are given a direct semantics in terms of normative structures which makes our deontic modalities no longer interdefinable;

2. The action combinators are the standard $+$ and $\cdot$ but exclude the

[1] In SDL terminology the axioms translate as: K is $O(p \to q) \to (O(p) \to O(q))$; D is $O(p) \to P(p)$; T is $O(p) \to p$; N is $if p then O(p)$, where p is a propositional variable and O is the obligation modality and P is the permission modality applied over propositions. Note that O and P are dual and play the role of $\Box$ and $\Diamond$ respectively.

[2] As in modal logis in SDL all modalities can be defined in terms of only one of them; take now O to be the principal modality then $P(p) = \neg O(\neg p)$ and $F(p) = O(\neg p)$.

Kleene * and add a concurrency operator $\times$ which addopts the synchrony model of R. Milner's SCCS [Mil83];

3. An action negation operation is defined to encode violation of an obligation. Obligations (prohibitions) can be violated by not doing the obligatory action (or doing the forbidden action);

4. The reparations for the contrary-to-duty obligations (CTDs) and for the contrary-to-prohibitions (CTPs) are included directly in the definition of the O and F modalities;

5. The definition and semantics of the deontic operators as given here excludes the most important SDL paradoxes and respects several natural properties which are found in legal contracts. One of the interesting properties relates to the concurrent execution of two actions: $O(\alpha) \wedge O(\beta) \rightarrow O(\alpha \times \beta)$.

The notion of *synchrony* has different meanings in different areas of computer science. Here we take the distinction between *synchrony* and *asynchrony* as presented in the SCCS calculus of [Mil83] and later implemented in e.g. the Esterel synchronous programming language [BG92, Ber00]. We understand *asynchrony* as when two concurrent systems proceed at indeterminate relative speeds (i.e. their actions may have different noncorelated durations); whereas in the *synchrony* model each of the two concurrent systems instantaneously perform a single action at each time instant.

The *perfectly synchronous concurrency model* takes the assumption that time is discrete and that basic actions are instantaneous (i.e. take zero time and represent the time step). Moreover, at each time step all possible actions are performed, i.e. the system is considered eager and active. For this reason if at a time point there is enabled an obligation to do an action then this action must be immediately executed so that the obligation is not violated. The reasoning is governed by the assumption of a global clock which provides the time unit for all the actors in the system. Note that for practical purposes this is a rather strong assumption which offends the popular relativistic view from process algebras [Mil95,Hoa85]. On the other hand the mathematical framework of the synchronous calculus is much cleaner and more expressive than the asynchronous model, and the experience of the Esterel implementation and use in industry contradict the general believe.

SCCS introduces synchronous composition operator $\times$ over processes which is different from the classical $\|$ of CCS. In SCCS the meaning of processes is given in a process algebra style and thus the structural operational semantics of $\times$ is:

$$\frac{P \xrightarrow{a} P' \qquad Q \xrightarrow{b} Q'}{P \times Q \xrightarrow{ab} P' \times Q'}$$

$$\begin{array}{lcl} \alpha & := & a \mid \mathbf{0} \mid \mathbf{1} \mid \alpha + \alpha \mid \alpha \cdot \alpha \mid \alpha \times \alpha \\ \mathcal{C} & := & \phi \mid O_{\mathcal{C}}(\alpha) \mid P(\alpha) \mid F_{\mathcal{C}}(\alpha) \mid \mathcal{C} \to \mathcal{C} \mid \bot \end{array}$$

Table 1: Syntax of the deontic logic with synchrony.

We adopt the synchrony model and add synchronous (or concurrent) composition as an action combinator with slight differences than that of SCCS. This models the fact that two or more actions are *done at the same time*.

The technical discourse of the paper presents first the actions and their interpretation as trees. Then it defines the models over which we interpret the deontic modalities. The semantics of the modalities relies on the interpretation of the actions in order to search the state space of the model. Particular properties of the deontic operators are presented in the end. Moreover, a proof of the tree model property is presented for our semantics.

2 Syntax and Semantics

None of the few papers that consider repetition (i.e. Kleene *) as an action combinator under deontic modalities [vdM96, BWM01] do not give a precise motivation for having such recurring actions inside obligations, permissions, or prohibitions. Experience provides us examples which are counter intuitive: take the expression $O(a^*)$ - "One is obliged to not pay, or pay once, or pay twice in a row, or..." - which puts no actual obligations; or take $P(a^*)$ - "One has the right to do any sequence of action a." - which is a very shallow permission and is captured by the widespread *Closure Principle* in jurisprudence where *what is not forbidden is permitted* [Seg82]. Moreover, as pointed out in [BWM01] expressions like $F(a^*)$, $P(a^*)$ should be simulated with the PDL modalities by respectively $\langle a^* \rangle F(a)$, $[a^*]P(a)$. In our opinion the * combinator under deontic modalities can be captured by using temporal or dynamic logic modalities along with deontic modalities over actions. We defer the presentation of such combination to another paper and concentrate here only on the properties of the deontic modalities alone.

We do not consider the Kleene * operator over the actions inside the deontic modalities. The syntax of the deontic logic with synchrony is given by the grammar in Table 1.

2.1 Actions

Definition 2.1 *Consider a finite set of* basic *(or atomic) actions $\mathcal{A}_B$ (denoted by $a, b, c, \ldots$). The special actions* **0** *and* **1** *are called respectively the* violating *action and the* skip *action. The action combinators are: "$+$" for* choice *of two actions, "$\cdot$" for* sequence *of two actions (or concatenation), "$\times$" for* concurrent composition *(synchronously) of two actions. We gener-*

(1) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$	(10) $\alpha \times (\beta \times \gamma) = (\alpha \times \beta) \times \gamma$
(2) $\alpha + \beta = \beta + \alpha$	(11) $\alpha \times \beta = \beta \times \alpha$
(3) $\alpha + \mathbf{0} = \mathbf{0} + \alpha = \alpha$	(12) $\alpha \times \mathbf{1} = \mathbf{1} \times \alpha = \alpha$
(4) $\alpha + \alpha = \alpha$	(13) $\alpha \times \mathbf{0} = \mathbf{0} \times \alpha = \mathbf{0}$
(5) $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$	(14) $a \times a = a \quad \forall a \in \mathcal{A}_B$
(6) $\alpha \cdot \mathbf{1} = \mathbf{1} \cdot \alpha = \alpha$	(15) $\alpha \times (\beta + \gamma) = \alpha \times \beta + \alpha \times \gamma$
(7) $\alpha \cdot \mathbf{0} = \mathbf{0} \cdot \alpha = \mathbf{0}$	(16) $(\alpha + \beta) \times \gamma = \alpha \times \gamma + \beta \times \gamma$
(8) $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$	(17) $(\alpha_\times \cdot \alpha) \times (\beta_\times \cdot \beta) = (\alpha_\times \times \beta_\times) \cdot (\alpha \times \beta)\ \forall \alpha_\times, \beta_\times \in \mathcal{A}_B^\times$
(9) $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$	

Table 2: Axioms of action equality.

ally call compound actions *(or just actions) terms of $\mathcal{A}$ (denoted $\alpha, \beta, \gamma, \ldots$) obtained from basic actions, $\mathbf{0}$, and $\mathbf{1}$ using the action combinators. We call* concurrent actions *and denote by $\mathcal{A}_B^\times \subset \mathcal{A}$ the subset of elements of $\mathcal{A}$ generated using only $\times$ constructor. The general representant of $\mathcal{A}_B^\times$ is written $\alpha_\times$. To avoid unnecessary parentheses we use the following precedence over the combinators: $+ < \cdot < \times$. Table 2 collects the axioms that define the equality between actions.*

Note that $\mathbf{0}, \mathbf{1} \notin \mathcal{A}_B^\times$. Also note that $\mathcal{A}_B^\times$ is finite because there is a finite number of basic actions in $\mathcal{A}_B$ which may be combined with the concurrency operator $\times$ in a finite number of ways (due to the idempotence of $\times$ over basic actions; see axiom (14)). Note the inclusion of sorts $\mathcal{A}_B \subseteq \mathcal{A}_B^\times \subset \mathcal{A}$. The axioms (1)-(4) define a commutative and idempotent monoid for the $+$. Axioms (5)-(7) define a monoid with a two sides annihilator element for the $\cdot$ sequence combinator. Axioms (8) and (9) give the distributivity of $\cdot$ over $+$. These give the algebraic structure of an idempotent semiring $(\mathcal{A}, +, \cdot, \mathbf{0}, \mathbf{1})$. Axioms (10)-(13) make $(\mathcal{A}, \times, \mathbf{1}, \mathbf{0})$ a commutative monoid with an annihilator element. Axioms (10) and (11) basically say that the syntactic ordering of actions in a concurrent action does not matter (the same as for choice $+$). Axiom (14) defines $\times$ to be idempotent over the basic actions $a \in \mathcal{A}_B$. Axioms (15) and (16) define the distributivity of $\times$ over $+$. From axioms (10)-(16) together with (1)-(4) we conclude that $(\mathcal{A}, +, \times, \mathbf{0}, \mathbf{1})$ is a commutative and idempotent semiring (NB. idempotence comes from (4), whereas (14) is an extra property of the semiring).

At this point we give an informal intuition for the elements (actions) of $\mathcal{A}$: we consider that the actions are performed by somebody (being that a person, a program, or an agent). We talk about "doing" and one should not think of *processes executing actions* and operational semantics like in SCCS; we do not discuss operational semantics nor bisimulation equivalences in this paper.

Definition 2.2 (demanding relation) *We call $<_\times$ the* demanding relation *and define it below. We say that β is more demanding than α iff*

$\alpha <_\times \beta$.

$$\alpha <_\times \beta \stackrel{\Delta}{=} \alpha \times \beta = \beta$$

We denote by $\leq_\times$ *the relation* $<_\times \cup =$*; i.e.* $\alpha \leq_\times \beta$ *iff either* $\alpha <_\times \beta$ *or* $\alpha = \beta$.

Note that the least demanding action is **1** (skiping means not doing any action). The basic actions are not related to each other by $<_\times$ and are the least demanding actions before **1**. It is routine to prove that the relation $<_\times|_{\mathcal{A}_B^\times}$ (i.e. $<_\times$ restricted to concurrent actions) is a partial order. Consider the following examples: $\mathbf{1} <_\times a$, $a <_\times a \times b$, $a <_\times a$, $a + b \not<_\times a + b$, $a \not<_\times b$, and $a \not<_\times b \times c$.

Proposition 2.1 *The relation* $<_\times|_{\mathcal{A}_B^\times}$ *is a partial order.*

Proof : For the relation $<_\times$ restricted to concurrent actions of $\mathcal{A}_B^\times$ the reflexivity is assured by the weak idempotence axiom (14). The transitivity and antisymmetry are immediate and moreover, they hold for the whole set $\mathcal{A}$ of actions; e.g. for *transitivity* take any $\alpha, \beta, \gamma \in \mathcal{A}$ s.t. $\alpha <_\times \beta$ and $\beta <_\times \gamma$. Then it is the case that from $\alpha \times \beta = \beta$ and $\beta \times \gamma = \gamma$ we get $\alpha \times \gamma = \alpha \times \beta \times \gamma = \beta \times \gamma = \gamma$ which is the desired conclusion $\alpha <_\times \gamma$ (note that we used the commutativity of the $\times$ operation and the transitivity of the equality of actions).

Note that reflexivity is not a property of the general actions, but only of the concurrent actions. Therefore, ireflexivity is not a property of the general actions either. For example $(a + b) \times (a + b) = a + b + a \times b$ but on the other hand $(a + b + a \times b) \times (a + b + a \times b) = a + b + a \times b$ due to the idempotence of the $\times$ over $\mathcal{A}_B$. Moreover, we can prove that for any action α there exists a fix point for the application of the $\times$ to the action itself. In other words, define $\beta_0 = \alpha$ and $\beta_i = \beta_{i-1} \times \alpha$, then $\exists n \in \mathbb{N}$ and $\exists j < n$ s.t. $\beta_j = \beta_n$. The proof uses the canonical representation of the action α. □

Proposition 2.2

1. *If* $\alpha_\times^1 <_\times \beta_\times^1 \wedge \cdots \wedge \alpha_\times^n <_\times \beta_\times^n$ *then* $\alpha_\times^1 \cdot \cdots \cdot \alpha_\times^n <_\times \beta_\times^1 \cdot \cdots \cdot \beta_\times^n \cdot \gamma$ *where* $\alpha_\times^i, \beta_\times^j \in \mathcal{A}_B^\times$ *and* $\gamma \in \mathcal{A}$.
2. *If* $\alpha_\times^i <_\times \beta_\times^j, \forall i \leq n, j \leq m$ *then* $(\alpha_\times^1 + \cdots + \alpha_\times^n) <_\times (\beta_\times^1 + \cdots + \beta_\times^m)$.

Proof : The proof for the first statement is based on axiom (17) whereas the proof of the second statement is based on the distributivity axioms (15) and (16) of $\times$ over $+$. □

As naturally found in legal contracts we take a *conflict relation* which is a priori given for the basic actions.

Definition 2.3 (conflict relation) *We consider a symmetric and irreflexive relation over the set of basic actions $\mathcal{A}_B$ which we call conflict relation and denote by $\#_{\mathcal{C}} \subseteq \mathcal{A}_B \times \mathcal{A}_B$. The converse relation of $\#_{\mathcal{C}}$ is the symmetric and reflexive compatibility relation which we denote by $\sim_{\mathcal{C}}$ and is defined as*

$$\sim_{\mathcal{C}} \triangleq \mathcal{U} \setminus \#_{\mathcal{C}}$$

where $\mathcal{U} = \mathcal{A}_B \times \mathcal{A}_B$ is the universal relation over basic actions.

The intuition of the conflict relation is that if two actions are in conflict then the actions cannot be executed concurrently. This intuition explains the need for the following equational implication:

$$(22) \quad a \#_{\mathcal{C}} b \rightarrow a \times b = \mathbf{0} \qquad \forall a, b \in \mathcal{A}_B.$$

The intuition of the compatibility relation is that if two actions are compatible then the actions can always be executed concurrently. There is *no transitivity* of $\#_{\mathcal{C}}$ or $\sim_{\mathcal{C}}$: In general, if $a \#_{\mathcal{C}} b$ and $b \#_{\mathcal{C}} c$, not necessarily $a \#_{\mathcal{C}} c$. This is natural as action b may be in conflict with both a and c but still $a \sim_{\mathcal{C}} c$.

Definition 2.4 (canonical form) *We say that an action α is in* canonical form *denoted by $\underline{\alpha}$ iff it has the following form:*

$$\underline{\alpha} = \sum_{i \in I} \alpha_{\times}^{i} \cdot \underline{\alpha^{i}}$$

where $\alpha_{\times}^{i} \in \mathcal{A}_B^{\times}$ and $\underline{\alpha^{i}} \in \mathcal{A}$ is an action in canonical form. The indexing set I is finite as the compound actions α are finite; i.e. there is a finite number of application of the $+$ operator. Actions $\mathbf{0}$ and $\mathbf{1}$ are in canonical form.

Theorem 2.3 *For every action α there exists a corresponding action $\underline{\alpha}$ in canonical form and equivalent to α.*

Proof : We use induction on the structure of the actions of $\mathcal{A}$ given by the combinators. In the inductive proof we take one case for each action construct. The proof also makes use of the axioms (1)-(17). For convenience in the presentation of the proof we define for an action in canonical form $\underline{\alpha}$ the set $R = \{\alpha_{\times}^{i} \mid i \in I\}$ to contain all the concurrent actions on the first "level" of $\underline{\alpha}$. Based on, we often use in the proof the alternative notation for the canonical form $\underline{\alpha} = +_{\alpha_{\times} \in R} \alpha_{\times} \cdot \underline{\alpha'}$ which emphasizes the exact set of the concurrent actions on the first level of the action $\underline{\alpha}$.

Basis:

a) If α is a basic action a of $\mathcal{A}_B$ it is immediately proven to be in canonical form just by looking at the definition of the canonical form. Action a is in canonical form with the set R containing only one element, namely a and the $\cdot$ combinator is applied to a and to skip action $\mathbf{1}$ ($a \cdot \mathbf{1} = a$). Note that we appeal to the common sense and the choice ($+$) of only one action ($+_a\, a$) should be understood as choice among action $\mathbf{0}$ and a ($+_a\, a \stackrel{def}{=} \mathbf{0} + a = a$).

b) The special actions $\mathbf{1}$ and $\mathbf{0}$ are considered by definition to be in canonical form.

In the inductive step we consider only one step of the application of the combinators; the general compound actions should follow from the associativity of the combinators.

Inductive steps:

a) If $\alpha = \beta + \beta'$ is a compound action obtained by applying once the $+$ combinator. By the induction hypothesis β and β' are in canonical form. It means that β should be $\beta = +_{b_i}\, b_i \cdot \beta_i$ and $\beta' = +_{b'_j}\, b'_j \cdot \beta'_j$.[3] Because of the associativity and commutativity of $+$, $\beta + \beta'$ is also in canonical form:

$$\beta + \beta' = \underset{b_i \in B}{+}\, b_i \cdot \beta_i \;+\; \underset{b'_j \in B'}{+}\, b'_j \cdot \beta'_j = \underset{a \in B \cup B'}{+}\, a \cdot \beta_a$$

where a and β_a are related in the sense that if $a = b_i$ then $\beta_a = \beta_i$ and if $a = b'_j$ then $\beta_a = \beta'_j$. Because the inductive hypothesis states that all β_i and β'_j are in canonical form it follows that also β_a (which is just a change of notation) are in canonical form.

b) If $\alpha = \beta \cdot \beta'$ with $\beta = +_{b_i}\, b_i \cdot \beta_i$ and $\beta' = +_{b'_j}\, b'_j \cdot \beta'_j$ in canonical form. We now make use of the distributivity of $\cdot$ over $+$, and of the associativity of $\cdot$ and $+$ combinators. α transforms in several steps into a canonical form. In the first step α is:

$$\alpha = \beta \cdot \beta' = (\underset{b_i \in B}{+}\, b_i \cdot \beta_i) \;\cdot\; (\underset{b'_j \in B'}{+}\, b'_j \cdot \beta'_j)$$

and if we consider $|B| = m$ then α becomes:

$$\alpha = b_1 \cdot \beta_1 \cdot (\underset{b'_j \in B'}{+}\, b'_j \cdot \beta'_j) \;+\; \ldots \;+\; b_m \cdot \beta_m \cdot (\underset{b'_j \in B'}{+}\, b'_j \cdot \beta'_j)$$

[3] Note that in the proof we consider only basic actions $b_i \in \mathcal{A}_B$ instead of concurrent actions from $\mathcal{A}_B^{\times}$ for the sake of a simpler presentation and notation; the proof for the general case with concurrent actions should be a straight forward generalization of what is presented here.

Subsequently α distributes the $\cdot$ over all the members of the choice actions. In the end α becomes a choice of sequences; when we consider $|B| = m$ and $|B'| = k$.

$$\alpha = b_1 \cdot \beta_1 \cdot b'_1 \cdot \beta'_1 \ + \ \ldots \ + \ b_m \cdot \beta_m \cdot b'_k \cdot \beta'_k$$

This is clearly a canonical form because all actions $\beta_i \cdot b'_j \cdot \beta'_j$ are in canonical form due to the inductive hypothesis.

c) If $\alpha = \beta \times \beta'$ with $\beta = +_{b_i} b_i \cdot \beta_i$ and $\beta' = +_{b'_j} b'_j \cdot \beta'_j$ in canonical form. The proof of this case is fairly lengthy and we show here only a simple particular case.

Let us consider actions $\beta = b \cdot \beta'$, $\gamma = c \cdot \gamma'$, and $\delta = d \cdot \delta'$ in canonical form. They are the components of $\alpha = (\beta + \gamma) \times \delta$. We apply the distributivity of $\times$ with respect to $+$ and get:

$$\alpha = \beta \times \delta + \gamma \times \delta = (b \cdot \beta') \times (d \cdot \delta') + (c \cdot \gamma') \times (d \cdot \delta')$$

By applying equation (17) we get:

$$\alpha = b \times d \cdot \beta' \times \delta' + c \times d \cdot \gamma' \times \delta'$$

This shows that α is in canonical form because by the inductive supposition $\beta' \times \delta'$ and $\gamma' \times \delta'$ are in canonical form.

□

For the deontic modalities one important notion is that of *action negation*. Action negation encodes the violation of an obligation. There have been a few works related to negation of actions for PDL-like logics [Mey88, HKT00, LW04, Bro03]. In [Mey88], the same as in [HKT00] action negation is with respect to the universal relation which for PDL gives undecidability. Decidability of PDL with negation of only atomic actions has been achieved in [LW04]. A so called "relativized action complement" is defined in [Bro03] which is the complement of an action (not w.r.t. the universal relation but) w.r.t. a set formed of atomic actions closed under the application of the action operators. This kind of negation still gives undecidability when several action operators are involved.

A natural and useful view of *action negation* is to say that the negation $\overline{\alpha}$ of action α is the action given by all the immediate actions that *take us outside* the tree of α. With $\underline{\alpha}$ it is easy to formally define $\overline{\alpha}$.

Definition 2.5 (action negation) *The* action negation *is a derived operator denoted by* $\overline{\alpha}$ *and is defined as a function* $\overline{\ } : \mathcal{A} \to \mathcal{A}$ *(i.e. action*

negation is not a principal combinator for the actions) which works on the equivalent canonical form $\underline{\alpha}$ *as:*

$$\overline{\alpha} = \overline{\underset{i\in I}{+}\ \alpha^i_\times \cdot \underline{\alpha^i}} = \underset{\beta_\times \in \overline{R}}{+} \beta_\times \ + \ \underset{j\in J}{+}\ \gamma^j_\times \cdot \overline{\underset{i\in I'}{+}\ \underline{\alpha^i}}$$

Consider $R = \{\alpha^i_\times \mid i \in I\}$. *The set* $\overline{R}$ *contains all the concurrent actions* $\beta_\times$ *with the property that* $\beta_\times$ *is not more demanding than any of the actions* $\alpha^i_\times$*:*

$$\overline{R} = \{\beta_\times \mid \beta_\times \in \mathcal{A}^\times_B \text{ and } \forall i \in I, \alpha^i_\times \not\leq_\times \beta_\times\},$$

and $\gamma^j_\times \in \mathcal{A}^\times_B$ *and* $\exists \alpha^i_\times \in R$ *s.t.* $\alpha^i_\times \leq_\times \gamma^j_\times$. *The indexing set* $I' \subseteq I$ *is defined for each* $j \in J$ *as:*

$$I' = \{i \in I \mid \alpha^i_\times \leq_\times \gamma^j_\times\}.$$

The negation operation formalizes the fact that an action is not performed. In an active system this boils down to performing the action given by $\overline{\alpha}$. In other words *not performing* action α means either not performing any of its immediate actions $\alpha^i_\times$, or by performing one of the immediate actions and then not performing the remaining action. Note that to perform an action $\alpha^i_\times$ means to perform any action that includes $\alpha^i_\times$ (this is encoded by the demanding relation $<_\times$). Therefore in the negation we may have actions $\gamma^j_\times$ which include more immediate actions, e.g. $\alpha = a \cdot b + c \cdot d$ and may perform $\gamma^j_\times = a \times c$. At this point we need to look at both actions b and d in order to derive the negation, e.g. performing now d means that α was done, whereas performing c means that α was not done (and $a \times c \cdot c$ must be part of negation).

Note that because $\mathcal{A}^\times_B$ is finite then we have finite sumation in the action negation; the maximum number of summands being at most $|\mathcal{A}^\times_B|$.

It was shown in [Pri08b] that the system of equations of Table 2 can be associated a convergent (i.e. terminating and confluent) term rewriting system. Therefore the system has the *normal form property* which means that for any action term we can find an equivalent action which cannot be further reduced using the reduciton rules. In other words, for an action α we can characterize the equivalence class of α (i.e. the set of all the actions that are equivalent with α by the axiomatic system of Table 2) with the normal form action $\alpha!$. Therefore, we know that there exists a unique normal form for actions, but we cannot pin-point it syntactically (so that to know how the unique normal form looks like). For the present work we are not so much interested in the normal form but in a slightly weaker notion of *almost normal form*.

It was noted in [Pri08a] that action negation is not independent of the representation. This basically means that applied to two equivalent actions the negation may yield not equivalent actions. This is not good and the problem, as noted in [Pri08a], comes from the fact that the canonical form

on which the action negation is applied is not unique. We cannot apply action negation to the unique normal form because we do not have a syntactic characterization of this normal form. Therefore still the action negation cannot be applied to a unique action equivalent to the action which is negated.

The results on the existence of the unique normal form and the observations in the proof of the negative of the independence of the representation for $\overline{\ }$ lead the way to the development of the *almost normal form* notion in what we present now. We prove that the canonical form which is also an almost normal form is *unique*. Moreover, we know exactly how this looks like: it is a canonical form with the restrictions as in Theorem 2.4. The most important restrictions are 3 and 4 which take care of the special actions $\mathbf{1}$ and $\mathbf{0}$. Therefore if the action negation is applied, in the same way as in the Definition 2.5, on a canonical form which is also an almost normal form then the uniqueness of the result is guaranteed (and all the proofs become easier).

Definition 2.6 (almost normal form) *If we can apply to an action α only axiom (8) (and none other of the axioms of Table 2) we call the action an* almost normal form*, and denote it $\underline{\alpha!}$.*

To apply an axiom means to apply the rule obtained from directing the axiom from left to right; see [Pri08b, BN98] for details on rewriting theory. The next two theorems relate the almost normal form with the canonical form and with the normal form of an action.

Theorem 2.4 *A canonical form $\underline{\alpha} = +_{i\in I}\ \alpha^i_\times \cdot \underline{\alpha^i}$ is an almost normal form of an action α iff it respects the following restrictions:*

1. *$\forall i \in I, \forall a \in \mathcal{A}_B$ then $\alpha^i_\times$ does not contain twice the same action a;*
2. *$\forall i, j \in I,\ \alpha^i_\times \neq \alpha^j_\times$;*
3. *$\forall i \in I$, either*
   (a) *$\underline{\alpha^i} \in \mathcal{A} \setminus \{\mathbf{0}, \mathbf{1}\}$ or*
   (b) *$\underline{\alpha^i}$ does not exist and in this case $\alpha^i_\times \in \mathcal{A}^\times_B \cup \{\mathbf{1}\}$ is allowed to be also $\mathbf{1}$;*
4. *$\underline{\alpha^i}$ respects strictly the restrictions 1, 2, and 3.*

Proof : We need to prove that none of the axioms of Table 2 except (8) can be applied to an action in canonical forms with the restrictions of the theorem; therefore the aciton is an almost normal form as in Definition 2.6. Note first that we work modulo associativity and commutativity for $+$ and $\times$, and modulo associativity for $\cdot$; this is allready from the canonical

form. Therefore we need to look at the remaining axioms of Table 2; but we consider their directed rule form (i.e. directed left to right). The following axioms need not be checked as they are dealt with by the canonical form directly: (6) right part, (7) right part, (9), (12), (13), (15), (16), (17). The main purpose of the canonical form is to make sure that the axioms for $\times$ (like (13), (15), (16), (17)) are applied exhaustively to the original action, and cannot be applied any more to the canonical form. In other words the axioms (15), (16), (17) push the $\times$ inside the action until it reaches the basic actions.

It remains to check: (3), (4), (6) left part, (7) left part, (14).

Rule (14) is taken care of by the first condition of the theorem and therefore this cannot be applied. Rule (4) is dealt with by the second condition. Rules (3) and (7) left part cannot be applied because of the third constraint (and the forth one for recursion) because of which $\mathbf{0}$ does not appear any more. Rule (6) left part cannot be applied because of the third constraint which makes $\underline{\alpha^i} \neq \mathbf{1}$. □

Theorem 2.5 *The normal form of an action α is obtained from the almost normal form $\underline{\alpha!}$ by a finite application of axioms (8) and (6).*

Proof : Clearly to an almost normal form the only axiom immediately applicable is (8). From this it may result an action which ends in a $\mathbf{1}$ (like $\alpha \cdot (\mathbf{1} + \beta) = \alpha \cdot \mathbf{1} + \alpha \cdot \beta$). So we can apply further the left part of axiom (6). No other way of applying the axioms is possible after one application of (8). □

Corollary 2.6 *The canonical form which is also an almost normal form of an action α is* unique *(modulo associativity and commutativity).*

We call a canonical form which is also an almost normal form a *canonical almost normal form* and we abreviate it by c.a.n.f.. The corollary is imediate from the proof of Theorem 2.4. There is no application of the axioms to a canonical almost normal form which yelds another canonical almost normal form.

Theorem 2.7 $\overline{\mathbf{1} + \alpha} = \mathbf{0},\ \forall \alpha \in \mathcal{A}$

Proof: The proof is by structural induction on the structure of α.

Basis: When $\alpha = \mathbf{0}$ or $\alpha = \mathbf{1}$ the proof is finished due to the convention $\overline{\mathbf{1}} = \mathbf{0}$ and the idempotence of $+$ and that $\mathbf{0}$ is a unity elemnt for $+$. When $\alpha = a, \forall a \mathcal{A}_B$ then by the definition $\overline{\mathbf{1} + a} = \mathbf{0} + \ \gamma_\times \cdot \overline{\mathbf{1}}$, $\forall \gamma_\times \in \mathcal{A}_B^\times$, which is equivalent to $\mathbf{0}$. It is clear that the first part of the negation is $\mathbf{0}$ because there is no action $\beta_\times \in \mathcal{A}_B^\times$ for which $\mathbf{1} \not\sqsubseteq \beta_\times$. In the second part of the

negation it is natural to have all the concurent actions $\gamma_\times$ as all of them include $\mathbf{1}$. Moreover, the action that needs to follow the sequence operator, i.e. $\overline{+_{i\in I'}\underline{\alpha^i}}$ is actually $\mathbf{1}$. Now by appling the fact that $\overline{\mathbf{1}} = \mathbf{0}$ and that $\mathbf{0}$ is the anihilator element for $\cdot$ we get our conclusion.

Inductive step: We do not need to consider the case when $\alpha = \alpha_1 \times \alpha_2$ because of the canonical form of the actions. We may only need to consider when $\alpha \in \mathcal{A}_B^\times$, i.e. $\alpha = a \times b \times \ldots$ but this is the same as in the basic case for basic actions that we considered before.

For when $\alpha = \alpha_\times^1 \cdot \alpha^1$ then we have as before $\overline{\mathbf{1} + \alpha_\times^1 \cdot \alpha^1} = \mathbf{0} + \gamma_\times \cdot \overline{\mathbf{1} + \alpha^1}$. By the inductive hypothesis $\overline{\mathbf{1} + \alpha^1} = \mathbf{0}$ and as before the final result is $\mathbf{0}$.

For when $\alpha = \alpha_\times^1 \cdot \alpha^1 + \alpha_\times^2 \cdot \alpha^2$, as in the previous cases the negation is $\mathbf{0} + \gamma_\times \cdot \overline{\mathbf{1} + \alpha^1 + \alpha^2}$ or small variations depending on $\gamma_\times$. By the inductive hypothesis $\overline{\mathbf{1} + \alpha^1 + \alpha^2} = \mathbf{0}$ and we have our conclusion. □

Definition 2.7 (rooted tree) *A* rooted tree *is an acyclic connected graph* $(\mathcal{N}, \mathcal{E})$ *with a designated node* r *called* root *node.* $\mathcal{N}$ *is the set of* nodes *and* $\mathcal{E}$ *is the set of* edges *(where an edge is an ordered pair of nodes* (n, m)*). We consider* rooted trees with labeled edges *and denote the labeled directed edges with* (n, α, m) *and the tree with* $(\mathcal{N}, \mathcal{E}, \mathcal{A}_B)$*. The labels* $\alpha \in 2^{\mathcal{A}_B}$ *are* sets of basic labels*; e.g.* $\alpha_1 = \{a, b\}$ *or* $\alpha_2 = \{a\}$ *with* $a, b \in \mathcal{A}_B$*. Labels are compared for set equality (or set inclusion). Note the special* empty set *label. We consider a special label* Λ *to stand for an impossible label. We restrict our presentation to* finite *rooted trees (i.e., there is no infinite path in the graph starting from the root node). The set of all such defined trees is denoted* $\mathcal{T}$*.*

Notation: When the label of an edge is not important (i.e. can be any label) we may use the notation (n, m) instead of (n, α, m) $\forall \alpha \in 2^{\mathcal{A}_B}$. All nodes $\{m \,|\, (n, m)\}$ are called the *children* nodes of n. The *siblings* of a node m are all the nodes which have common parent with m; i.e. $sibl(m) = \{m' \,|\, (n, m), (n, m') \in \mathcal{E}\}$. Note that the root node has no siblings. We use the notation $T_n \subseteq T$ to denote the *subtree* of T with root in the node n of T. We denote by $|n|$ the *depth* of the node n in the tree; which is the numaber of transitions needed to reach n from the root. A path of a tree is denoted $\sigma \in T$. A path which cannot be extended with a new transition is called *final*. The final nodes on each final path are called *leaf nodes*; denote by $leafs(T) = \{n \mid n \text{ is a leaf node}\}$. The *hight* of a tree, denoted $h(T)$, is the maximum of $|n|$ for all the leaf nodes n.

Definition 2.8 (tree isomorphism) *Two trees* $T_1 = (\mathcal{N}_1, \mathcal{E}_1, \mathcal{A}_1)$ *and* $T_2 = (\mathcal{N}_2, \mathcal{E}_2, \mathcal{A}_2)$ *are isomorphic, denoted* $T_1 \doteq T_2$*, iff* $\mathcal{A}_1 = \mathcal{A}_2$ *(the labels are the same), and there is a bijective function* $rn : \mathcal{N}_1 \to \mathcal{N}_2$ *s.t.* $rn(root_1) = root_2$ *and* $\forall (n, \alpha, m) \in \mathcal{E}_1$ *then* $(rn(n), \alpha, rn(m)) \in \mathcal{E}_2$*.*

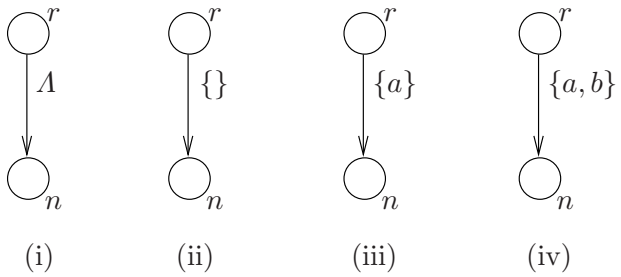

Figure 1: Trees corresponding to $\mathbf{0}$, $\mathbf{1}$, $a \in \mathcal{A}_B$, and $a \times b \in \mathcal{A}_B^{\times}$.

Theorem 2.8 (interpretation of actions) *For any action α there exists a tree representation corresponding to the canonical almost normal form $\underline{\alpha!}$.*

Proof: The *representaiton* is an interpretation function $I : \mathcal{A} \to \mathcal{T}$ which interprets all action terms as trees. More precisely, when given an arbitrary action of $\mathcal{A}$ the canonical almost normal form is computed first and then I generates the tree representation of the canonical form. We do not give an algorithm for computing the canonical almost normal form as one may simply do an exhaustive applicaiton of the axioms excluding (8).

The function I is defined inductively. The basis is to interpret each concurrent action of $\mathcal{A}_B^{\times}$ as a tree with labeled edges from $2^{\mathcal{A}_B}$ as pictured in Fig.1. Note that actions of $\mathcal{A}_B^{\times} \cup \{\mathbf{0}, \mathbf{1}\}$ are in canonical form. For a general action in canonical form $\underline{\alpha} = +_{i \in I} \ \alpha_{\times}^i \cdot \underline{\alpha^i}$ the tree is generated by adding one branch to the root node for each element $\alpha_{\times}^i$ of the top summation operation. The label of the branch is the set $\{\alpha_{\times}^i\}$ corresponding to the concurrent action. The construction continues inductively by attaching at the end of each newly added branch the tree interpretation of the smaller action $\underline{\alpha^i}$. Intuitively, $+$ provides the branching in the tree, and $\cdot$ provides the parent-child relation on each branch. □

Henceforth we work only with the canonical almost normal form because it is unique. We also work with the unique tree representation $I(\alpha)$. Associated to each tree is its linearization; which is the set of all the labeled full paths in the tree. This set of sequences of sets of basic actions is also unique. In [Pri08a] was proven the completeness of the axiom system of Table 2 w.r.t. regular sets of concurrent strings, which are exactly sets of sequences of sets of basic actions. Because of the completeness we have that $\alpha = \beta$ iff $I(\alpha) \doteq I(\beta)$; if the trees interpreting two actions are isomorphic (i.e. denote the same tree) then the actions are equal. Therefore instead of working with the trees we can work with the actions.

2.2 Semantics

The expressions $\mathcal{C}$ of the logic are given a model theoretic semantics in terms of *normative structures*. An expression may be a propositional constant (or assertion) ϕ drawn from a finite set Φ_B, an implication $\rightarrow$ of two expressions, the propositional constant $\bot$ (standing for *false*), and the deontic modalities. The operators $\wedge, \vee, \neg, \leftrightarrow, \top$ are defined from $\rightarrow$ and $\bot$ as in propositional logic.

$O_{\mathcal{C}}(\alpha)$, $P(\alpha)$, and $F_{\mathcal{C}}(\alpha)$ represent respectively the obligation, permission, and prohibition of performing a given *action* α. Intuitively $O_{\mathcal{C}}(\alpha)$ states the obligation to do α, and the *reparation* $\mathcal{C}$ in case the obligation is *violated*, i.e. whenever α is not performed. Particularly the modality $O_{\mathcal{C}}(\alpha)$ (resp. $F_{\mathcal{C}}(\alpha)$) represents what is called CTD (resp. CTP) in the deontic logic community. The reparation may be any contract clause. Obligations without reparations $O_{\bot}(\alpha)$ are usually written as $O(\alpha)$ (we use the same notation when the reparation $\mathcal{C}$ is not important). The prohibition modality $F_{\mathcal{C}}(\alpha)$ states the actual forbearing of the action $F(\alpha)$ together with the reparation $\mathcal{C}$ in case the prohibition is violated. Note that it is possible to express nested CTDs and CTPs.

Definition 2.9 (normative structure) *A* labeled Kripke structure *is a structure* $K = (\mathcal{W}, R_{2^{\mathcal{A}_B}}, \mathcal{V})$ *where* $\mathcal{W}$ *is a set of* worlds *(states),* $\mathcal{V} : \Phi_B \rightarrow 2^{\mathcal{W}}$ *is a* valuation function *of the propositional constants returning a set of worlds where the constants hold.* $\mathcal{A}_B$ *is a finite set of* basic labels*,* $2^{\mathcal{A}_B}$ *is the powerset representing the* labels *of the structure, and* $R_{2^{\mathcal{A}_B}} : 2^{\mathcal{A}_B} \rightarrow 2^{\mathcal{W}\times\mathcal{W}}$ *is a function returning for each label a relation on the set of worlds. In a* deterministic *labeled Kripke structure the function* $R_{2^{\mathcal{A}_B}}$ *associates to each label a partial function instead of a relation, therefore for each label from one world there is at most one reachable world. A* normative structure *is a deterministic labeled Kripke structure with a marking function* $\varrho : \mathcal{W} \rightarrow 2^{\Psi}$ *which marks each state with one or several markers from* $\Psi = \{\circ_a, \bullet_a \mid a \in \mathcal{A}_B\}$*. The marking function respects the restriction that no state can be marked by both* $\circ_a$ *and* $\bullet_a$ *at the same time (for any* $a \in \mathcal{A}_B$*). Normative structures are denoted* $N = (\mathcal{W}, R_{2^{\mathcal{A}_B}}, \mathcal{V}, \varrho)$*. A* pointed normative structure *is a normative structure with a designated state* i*, and is denoted by* N, i*.*

We denote by an indexed t a node of a tree (or by r the root) and by an indexed s (or i for initial) a state of a normative structure. Henceforth we use the more graphical notation $t \xrightarrow{\alpha} t'$ ($s \xrightarrow{\alpha} s'$) for an edge (transition) in a tree (normative structure) instead of the classical one (t, α, t') ($(s, s') \in R_{2^{\mathcal{A}_B}}(\alpha)$) that we had before. Note that we consider both the trees and the normative structures to have the same set of basic labels $\mathcal{A}_B$ (which correspond to the basic actions). We use deterministic structures because in the deontic realm (e.g. legal contracts) each action must have a well determined behavior (i.e. the actions do not have a nondeterministic

outcome). The deterministic restriction of Kripke structures has been investigated in [BAHP81] where an EXPTIME decision procedure is given for the satisfiability problem of PDL interpreted over deterministic structures. The marking function and the markers are needed to identify obligatory (i.e. $\circ$) and prohibited (i.e. $\bullet$) actions. Markers with similar purposes have been used in [Mey88] to identify violations of obligations, in [vdM96] to mark permitted transitions, and in [CM] to identify permitted events.

Definition 2.10 (simulation) *For a rooted tree $T = (\mathcal{N}, \mathcal{E}, \mathcal{A}_B)$ and a normative structure $N = (\mathcal{W}, R_{2^{\mathcal{A}_B}}, \mathcal{V}, \varrho)$ we define a relation $\mathcal{S} \subseteq \mathcal{N} \times \mathcal{W}$ which we call the* simulation *of the tree node by the state of the structure.*
$t \mathcal{S} s$ iff $\forall t \xrightarrow{\gamma} t' \in T$, $\exists s \xrightarrow{\gamma'} s' \in N$ s.t. $\gamma \subseteq \gamma'$ and $t' \mathcal{S} s'$ and
$\forall s \xrightarrow{\gamma'} s' \in N$ with $\gamma \subseteq \gamma'$ then $t' \mathcal{S} s'$.
We say that a tree T, with root r is simulated by a normative structure N with respect to a state s, denoted $T \mathcal{S}_s N$, iff $r \mathcal{S} s$.

Note two differences with the classical definition of simulation: first, the labels of the normative structure may be bigger than the labels in the tree because respecting an obligatory action means executing an action which incorporates (is bigger than) it. We can drop this condition and consider only $\gamma = \gamma'$, in which case we call the relation *strong simulation* and denote by $\hat{\mathcal{S}}$. Second, any transition in the normative structure that can simulate an edge in the tree is said to respect the action denoted by the edge. From this state onwards we need to be able to continue to look in the structure for the remaining tree (to see if it is respected) and therefore the transition must enter under the simulation relation. We can weaken the definition by combining this condition with the one before into: $\forall t \xrightarrow{\gamma} t' \in T, \forall s \xrightarrow{\gamma'} s' \in N$ with $\gamma \subseteq \gamma'$ then $t' \tilde{\mathcal{S}} s'$. We call the resulting relation *partial simulation* and denote it by $\tilde{\mathcal{S}}$.

Definition 2.11 (maximal simulating structure) *Whenever $T \mathcal{S}_i N$ then we call the* maximal simulating structure w.r.t. T and i, *and denote it by $N^{T,i}_{max} = (\mathcal{W}', R'_{2^{\mathcal{A}_B}}, \mathcal{V}', \varrho')$ the sub-structure of $N = (\mathcal{W}, R_{2^{\mathcal{A}_B}}, \mathcal{V}, \varrho)$ s.t.:*

1. *$i \in \mathcal{W}'$*
2. *$\mathcal{V}' = \mathcal{V}|_{\mathcal{W}'}$ and $\varrho' = \varrho|_{\mathcal{W}'}$*
3. *$\forall t \xrightarrow{\gamma} t' \in T$ then $\forall s \xrightarrow{\gamma'} s' \in N$ s.t. $t \mathcal{S} s \wedge \gamma \subseteq \gamma' \wedge t' \mathcal{S} s'$ do add s' to $\mathcal{W}'$ and add $s \xrightarrow{\gamma'} s'$ to $R'_{2^{\mathcal{A}_B}}$.*

We call the non-simulating reminder of N w.r.t. T and i *the sub-structure $N^{T,i}_{rem} = (\mathcal{W}'', R''_{2^{\mathcal{A}_B}}, \mathcal{V}'', \varrho'')$ of N s.t.: $s \xrightarrow{\gamma} s' \in R''_{2^{\mathcal{A}_B}}$ iff $s \xrightarrow{\gamma} s' \notin N^{T,i}_{max} \wedge s \in N^{T,i}_{max} \wedge \exists s \xrightarrow{\gamma} s'' \in N^{T,i}_{max}$; and $s \in \mathcal{W}''$ iff s is part of a transition in $N^{T,i}_{rem}$; and $\mathcal{V}'' = \mathcal{V}|_{\mathcal{W}''}$ and $\varrho'' = \varrho|_{\mathcal{W}''}$.*

$N, i \models \phi$ iff $i \in \mathcal{V}(\phi)$.
$N, i \not\models \bot$
$N, i \models \mathcal{C}_1 \to \mathcal{C}_2$ iff whenever $N, i \models \mathcal{C}_1$ then $N, i \models \mathcal{C}_2$.
$N, i \models O_{\mathcal{C}}(\alpha)$ iff $I(\alpha)\ \mathcal{S}_i\, N$, and
$\forall t \xrightarrow{\gamma} t' \in I(\alpha)$, $\forall s \xrightarrow{\gamma'} s' \in N$ s.t. $t\,\mathcal{S}\,s \wedge \gamma \subseteq \gamma'$
then $\forall a \in \mathcal{A}_B$ if $a \in \gamma$ then $\circ_a \in \varrho(s')$, and
$\forall s \xrightarrow{\gamma'} s' \in N^{I(\alpha),i}_{rem}$ then $\forall a \in \mathcal{A}_B$ if $a \in \gamma'$ then $\circ_a \notin \varrho(s')$, and
$N, s \models \mathcal{C}$ $\forall s \in N$ with $t\,\hat{\mathcal{S}}\,s \wedge t \in \mathit{leafs}(I(\overline{\alpha}))$.
$N, i \models F_{\mathcal{C}}(\alpha)$ iff $I(\alpha)\ \tilde{\mathcal{S}}_i\, N$ then
$\forall \sigma \in I(\alpha)$ a full path s.t. $\sigma\ \mathcal{S}_i\, N$,
$\exists t \xrightarrow{\gamma} t' \in \sigma$ s.t. $\forall s \xrightarrow{\gamma'} s' \in N$ with $t\,\mathcal{S}\,s \wedge \gamma \subseteq \gamma'$ then
$\forall a \in \mathcal{A}_B$ if $a \in \gamma'$ then $\bullet_a \in \varrho(s')$ and
$N, s \models \mathcal{C}$ $\forall s \in N$ with $t\,\mathcal{S}\,s \wedge t \in \mathit{leafs}(\sigma)$.
$N, i \models P(\alpha)$ iff $I(\alpha)\ \mathcal{S}_i\, N$, and
$\forall t \xrightarrow{\gamma} t' \in I(\alpha)$, $\forall s \xrightarrow{\gamma'} s' \in N$ s.t. $t\,\mathcal{S}\,s \wedge \gamma \subseteq \gamma'$
then $\forall a \in \mathcal{A}_B$ if $a \in \gamma$ then $\bullet_a \notin \varrho(s')$.

Table 3: Semantics for the deontic logic with synchronous actions.

Definition 2.12 (semantics) *We give in Table 3 a recursive definition of the* satisfaction relation $\models$ *of an expression $\mathcal{C}$ w.r.t. a normative structure N and a state i (or w.r.t. a pointed normative structure N, i); it is written $N, i \models \mathcal{C}$ and is read as "$\mathcal{C}$ is* satisfied *in the normative structure N at state i". We write $N, i \not\models \mathcal{C}$ whenever $\models$ is not the case. We say that "$\mathcal{C}$ is* globally satisfied *in N", and write $N \models \mathcal{C}$ iff $\forall s \in N,\ N, s \models \mathcal{C}$. A formula is* satisfiable *iff $\exists N, \exists s \in N$ s.t. $N, s \models \mathcal{C}$. A formula is* valid *(denoted $\models \mathcal{C}$) iff $\forall N, N \models \mathcal{C}$.*

The propositional connectives have the classical semantics. More interesting and particular to our logic is the interpretation of the deontic modalities. For the $O_{\mathcal{C}}$ the semantics has basically two parts: the second part is just the last line and states that if the obligation is violated (i.e. $\overline{\alpha}$ negation of the action is performed) then the reparation $\mathcal{C}$ should hold. This definition is similar to the definition of the box modality of PDL only that here it is applied to the negation of the action (i.e. it looks only at the leafs and it uses strong simulation to have exactly the same labels as the action tree). The first part of the semantics is the interpretation of the obligation. The first line says how to walk on the structure depending on the tree of the action α. The simulation relation is used because in the structure there may be transitions labeled with more demanding actions which intuitively if we do these actions then the obligation of α is still respected. The simulation relation also takes care that all the choices of an action appear as transitions in the structure. The second and third lines mark all the transi-

tions (their ending states) of the structure which simulate edges in the tree with markers $\circ_a$ corresponding to the labels of the simulated edge. This is need both for the proof of the main property $(O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta) \rightarrow O_{\mathcal{C}}(\alpha \times \beta))$ and also in proving $O_{\mathcal{C}}(\alpha) \rightarrow \neg F_{\mathcal{C}}(\alpha)$ which relates obligations and prohibitions in Proposition 3.1. Line four ensures that no other reachable relevant transitions of the structure are marked with obligation markers $\circ$. This is essential in the proof of the key Lemma 3.5 of the main result of Theorem 3.4.

For the $F_{\mathcal{C}}$ modality we use partial simulation $\tilde{\mathcal{S}}_i$ in order to have our intuition that if an action is not present as a label of an outgoing transition of the model then the action is *by default* considered forbidden. In the second line we consider *all* paths in order to respect the intuition that $F(a + b) = F(a) \wedge F(b)$, prohibition of a choice must prohibit all. In the third line we consider just the *existence* of an edge on each full path in order to respect the intuition that forbidding a sequence means forbidding some action on that sequence. Note that we are interested only in *full* paths simulated by the structure because for the other paths some of the transitions are missing and thus there is some action on the sequence which is forbidden. For this chosen edge we look for all the transitions of the normative structure from the chosen node which have a label *more demanding* than the label of the edge; this is in order to respect the intuition that $F(a) \Rightarrow F(a \times b)$, forbidding an action implies forbidding any action more demanding. The last line states that if the prohibition is violated then the reparation $\mathcal{C}$ must hold in the states where the violation is observed.

For the semantics of P we specify that $\bullet$ markers should not be present in order to capture the principle that *what is not forbidden is permitted*. The semantics of O, P, or F relates to the trace-based semantics of Process Logic [Pra79] and to some extent to the modalities of [vdM96].

3 Properties of the Deontic Operators

The semantics of the deontic operators is rather involved: it is based on an algebraic formalism for the actions which are interpreted as rooted trees; the information in the trees (compare to sets of traces [Pra79]) is used by the particular notion of simulation relation to know how to walk on the normative structure in the search of the markings which tell the truth value of the deontic modality. The rest of the complications in the semantics are necessary for capturing several intuitive properties of the deontic operators which we discuss in this section.

Proposition 3.1 *The following statements are true:*

$$\models \neg O_{\mathcal{C}}(\mathbf{0}) \quad (1)$$

$$\models O_{\mathcal{C}}(\mathbf{1}) \quad (2)$$

$$\models P(\alpha) \rightarrow \neg F_{\mathcal{C}}(\alpha) \quad (3)$$

$$\models O_{\mathcal{C}}(\alpha) \rightarrow P(\alpha) \quad (4)$$

$$\textit{if } \alpha = \beta \textit{ then } \models O_{\mathcal{C}}(\alpha) \leftrightarrow O_{\mathcal{C}}(\beta) \quad (5)$$

Proof : Note first that these statements for deontic modalities applied to actions are the correspondent of the well known statements over propositions which are the basis of SDL.

We give first quick proof arguments. For the first statement it suffices to notice that the tree interpreting $\mathbf{0}$ cannot be simulated by any normative structure because of the special label Λ which does not appear in the structure. For the second statement note that the tree interpreting $\mathbf{1}$ is trivially simulated by any normative structure. The proof of the third statement is based on the restriction on the marking function ϱ from Definition 2.9. The forth statement is immediate from the semantics and the same restriction on ϱ. The fifth statement is an inference rule and its proof takes into consideration all the axioms for the equality of actions from Table 2. The key is the fact that the semantics of O uses the trees generated from the *canonical* form of the actions and not from any action.

For the proof of $\models \neg O_{\mathcal{C}}(\mathbf{0})$ we need to show that there is no model which makes $O_{\mathcal{C}}(\mathbf{0})$ true. This is because of the definition of $\neg O_{\mathcal{C}}(\mathbf{0})$ as $O_{\mathcal{C}}(\mathbf{0}) \rightarrow \perp$ which is true only if $O_{\mathcal{C}}(\mathbf{0})$ is false. By *reductio ad absurdum* suppose that it exists a model which makes $O_{\mathcal{C}}(\mathbf{0})$ true. This means (by the definition of the semantics of O) that the tree interpreting $\mathbf{0}$ must be simulated by the model. But this is not possible because of the special label Λ appearing in the tree of $\mathbf{0}$ which does not appear in the labels of the normative structures.

For the statement $\models O_{\mathcal{C}}(\mathbf{1})$ take any normative structure. The tree interpreting $\mathbf{1}$ is trivially simulated by any normative structure because the only edge of the tree is labeled with the empty label and thus any transition of the structure simulates the edge. The second condition in the semantics of O is satisfied as there is no basic label a in the label of the edge. It is clear that any edge on the first level of the structure enters into the maximal simulating structure and therefore the non-simulating reminder $N_{rem}^{I(\mathbf{1}),i}$ is empty and the third condition is trivially satisfied. Because $\overline{\mathbf{1}} = \mathbf{0}$ then there is no state s to satisfy the requirements of the last condition and thus it is trivially satisfied too.

Note that $O_{\mathcal{C}}(\mathbf{1})$ is valid only in the *reflexive* structures. This means that the structures must satisfy the property that from each state there is a transition to itself.

For the proof of $\models O_{\mathcal{C}}(\alpha) \rightarrow P(\alpha)$ take an arbitrary pointed normative structure N, i which makes $O_{\mathcal{C}}(\alpha)$ true. This means that $I(\alpha)\ \mathcal{S}_i\, N$. This is the first part from the semantics of $P(\alpha)$. Moreover, from the semantics of $O_{\mathcal{C}}(\alpha)$ we have that $\forall t \xrightarrow{\gamma} t' \in \sigma$, $\forall s \xrightarrow{\gamma'} s' \in N$ s.t. $t\,\mathcal{S}\,s \wedge \gamma \subseteq \gamma'$ then $\forall a \in \gamma$ we have $\circ_a \in \varrho(s')$. Because of the restriction on the marking function we get $\forall a \in \gamma$ we have $\bullet_a \notin \varrho(s')$. This is the second requirement of the semntics for $P(\alpha)$.

For the proof of $\models P(\alpha) \rightarrow \neg F_{\mathcal{C}}(\alpha)$ we use *reductio ad absurdum* and suppose that it exists a pointed structure N, i which makes both $P(\alpha)$ and $F_{\mathcal{C}}(\alpha)$ true. It is easy to see that $\tilde{\mathcal{S}} \subseteq \mathcal{S}$ and therefore from the semantics of P we conclude that $I(\alpha)\ \tilde{\mathcal{S}}_i\, N$. Moreover, $\exists \sigma \in I(\alpha)$ s.t. $\sigma\ \mathcal{S}_i\, N$ (as in the semantics of F) and it exists also an edge $t \xrightarrow{\gamma} t' \in \sigma$ s.t. $\forall s \xrightarrow{\gamma'} s' \in N$ then $t\,\mathcal{S}\,s \wedge \gamma \subseteq \gamma'$. Take one of these transitions $s \xrightarrow{\gamma'} s' \in N$: from the semantics of $P(\alpha)$ we know that $\forall a \in \gamma$ then $\bullet_a \notin \varrho(s')$; from the semantics of $F_{\mathcal{C}}(\alpha)$ we know that $\forall a \in \gamma'$ then $\bullet_a \in \varrho(s')$. But this is a contradiction and the initial supposition is wrong and therefore (3) is true.

For the proof of (5) it is simple to notice that the semantics of O is based on the interpretation of the actions as trees. Therefore, because the actions are equal then the tree interpretation denotes the same tree (up to ismorphism). Thus, the semantics for $O_{\mathcal{C}}(\alpha)$ is the same as that for $O_{\mathcal{C}}(\beta)$ because they are working with the same tree $I(\alpha) \doteq I(\beta)$. □

The following corollary points out some other desirable tautologies that can be proven using the tautologies of Proposition 3.1.

Corollary 3.2 *The following statements are true:*

$$\models O_{\mathcal{C}}(\alpha) \rightarrow \neg F_{\mathcal{C}}(\alpha) \tag{6}$$

Proof: The proof of (6) can be obatained just from (4) and (3). Otherwize, we can prove the statement $\models O_{\mathcal{C}}(\alpha) \rightarrow \neg F_{\mathcal{C}}(\alpha)$ by using *reductio ad absurdum* and suppose that it exists a pointed structure N, i which makes both $O_{\mathcal{C}}(\alpha)$ and $F_{\mathcal{C}}(\alpha)$ true. It is easy to see that $\tilde{\mathcal{S}} \subseteq \mathcal{S}$ and therefore from the semantics of O we conclude that $I(\alpha)\ \tilde{\mathcal{S}}_i\, N$. Moreover, $\exists \sigma \in I(\alpha)$ s.t. $\sigma\ \mathcal{S}_i\, N$ (as in the semantics of F) and it exists also an edge $t \xrightarrow{\gamma} t' \in \sigma$ s.t. $\forall s \xrightarrow{\gamma'} s' \in N$ then $t\,\mathcal{S}\,s \wedge \gamma \subseteq \gamma'$. Take one of these transitions $s \xrightarrow{\gamma'} s' \in N$: from the semantics of $O_{\mathcal{C}}(\alpha)$ we know that $\forall a \in \gamma$ then $\circ_a \in \varrho(s')$; from the semantics of $F_{\mathcal{C}}(\alpha)$ we know that $\forall a \in \gamma'$ then $\bullet_a \in \varrho(s')$. On the other hand $\gamma \subseteq \gamma'$ and thus $\exists a \in \mathcal{A}_B$ s.t. $\circ_a, \bullet_a \in \varrho(s')$. But this is a contradiction with the restriction on the marking function ϱ from Definition 2.9. □

The following corollary points out conflicts that are avoided in the logic because of the semantics. These are natural requirements when reasoning about legal contracts.

Corollary 3.3 (conflicts) *The following statements are true:*

$$\models \neg(O_{\mathcal{C}}(\alpha) \wedge F_{\mathcal{C}}(\alpha)) \tag{7}$$

$$\models \neg(P(\alpha) \wedge F_{\mathcal{C}}(\alpha)) \tag{8}$$

$$\textit{if } \alpha \#_{\mathcal{C}} \beta \textit{ then } \models \neg(O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta)) \tag{9}$$

Proof: The proof of (7) follows by propositional resoning from (6) and the proof of (8) follows from (3). The proof of (9) follows from (1) and Theorem 3.4 as we show next. Because $\alpha \#_{\mathcal{C}} \beta$ then $\alpha \times \beta = \mathbf{0}$ and therefore $O_{\mathcal{C}}(\alpha \times \beta)$ is $O_{\mathcal{C}}(\mathbf{0})$. From Theorem 3.4 we get that $\models \neg(O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta)) \leftarrow \neg O_{\mathcal{C}}(\alpha \times \beta)$ and from the above we have that $\models \neg(O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta)) \leftarrow \neg O_{\mathcal{C}}(\mathbf{0})$. By *modus ponens* from (1) and the statement before we get $\models \neg(O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta))$. □

Theorem 3.4 (main property) $\models O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta) \rightarrow O_{\mathcal{C}}(\alpha \times \beta)$.

Before doing the proof of the theorem we give some helper results. First is an additional requirement to the semantics of the obligation which is needed to prove Lemma 3.8 and thus the theorem.

Definition 3.1 (fair obligations) *We call an obligation* fair *iff in addition to the semantics of Definition 2.12 the following* fairness constraint *is respected:*

$$\exists \gamma \textit{ s.t. } I(\alpha \times \gamma) \doteq TN^{I(\alpha),i}_{max} \tag{10}$$

Where $TN^{I(\alpha),i}_{max}$ is the tree unfolding of the structure $N^{I(\alpha),i}_{max}$ as in Lemma 4.1.

Lemma 3.5 *If $N, i \models O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta)$ then $N^{I(\alpha),i}_{max} = N^{I(\beta),i}_{max}$ otherwize $N^{I(\alpha),i}_{max} \subset N^{I(\beta),i}_{max}$ otherwize $N^{I(\alpha),i}_{max} \supset N^{I(\beta),i}_{max}$.*

Proof: Take an arbitrary pointed structure N, i and suppose $N, i \models O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta)$. The proof of this lemma uses *reductio ad absurdum* and is based on the fact that lines two and three in the semantics of obligation add $\circ$ markers to the states, and line four removes $\circ$ markers thus resulting in a contradiction.

If $N, i \models O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta)$ then $N, i \models O_{\mathcal{C}}(\alpha)$ and $N, i \models O_{\mathcal{C}}(\beta)$. From the first we have by the semantics that $I(\alpha)\ \mathcal{S}_i\ N$ which means that there exists the maximal simulating structure $N^{I(\alpha),i}_{max}$. From the semantics of $O_{\mathcal{C}}(\beta)$ we obtain similarly $N^{I(\beta),i}_{max}$. Both maximal simulating structures are substructures of the same N.

Suppose that there exists a transition $k \xrightarrow{\gamma} k' \in N^{I(\alpha),i}_{max}$ s.t. $k \xrightarrow{\gamma} k' \notin N^{I(\beta),i}_{max}$ and there is a transition $s \xrightarrow{\gamma'} s' \in N^{I(\beta),i}_{max}$ s.t. $s \xrightarrow{\gamma'} s' \notin N^{I(\alpha),i}_{max}$. Without loss of generality we will work with the transition $k \xrightarrow{\gamma} k'$ which

from the semantics of $O_{\mathcal{C}}(\alpha)$ we have that $\forall a \in \mathcal{A}_B$ if $a \in \gamma$ then $\circ_a \in \varrho(k')$. On the other hand the transition $k \xrightarrow{\gamma} k'$ is not part of $N_{max}^{I(\beta),i}$ and because $k \in N_{max}^{I(\beta),i}$ and we know that it exists at least one transition in $N_{max}^{I(\beta),i}$ (for example the transition $s \xrightarrow{\gamma'} s'$) then it means that $k \xrightarrow{\gamma} k' \in N_{rem}^{I(\beta),i}$. By the semantics of $O_{\mathcal{C}}(\beta)$ we know that $\forall a \in \mathcal{A}_B$ if $a \in \gamma$ then $\circ_a \notin \varrho(k')$. This results in a contradiction and therefore the initial supposition is wrong. □

Corollary 3.6

1. *If* $N_{max}^{I(\alpha),i} = N_{max}^{I(\beta),i}$ *then*
   (a) $TN_{max}^{I(\alpha),i} = TN_{max}^{I(\beta),i}$ *and*
   (b) $N_{rem}^{I(\alpha),i} = N_{rem}^{I(\beta),i}$.
2. *If* $N_{max}^{I(\alpha),i} \subset N_{max}^{I(\beta),i}$ *then*
   (a) $TN_{max}^{I(\alpha),i} \subset TN_{max}^{I(\beta),i}$ *and*
   (b) $\forall k \xrightarrow{\gamma} k' \in N_{rem}^{I(\alpha),i}$ *either* $k \xrightarrow{\gamma} k' \in N_{rem}^{I(\beta),i}$ *or* $k \xrightarrow{\gamma} k' \in N_{max}^{I(\beta),i}$.
3. *If* $N_{max}^{I(\alpha),i} \supset N_{max}^{I(\beta),i}$ *then*
   the same as before but interchange α *with* β.

Lemma 3.7 *For any* $\alpha, \beta, \gamma', \gamma'' \in \mathcal{A}$ *if* $I(\alpha \times \gamma') = I(\beta \times \gamma'') = T$ *then* $\exists \gamma''' \in \mathcal{A}$ *s.t.* $T = I(\alpha \times \beta \times \gamma''')$.

Proof: From the completeness result of the algebra of actions we get that because $I(\alpha \times \gamma') = I(\beta \times \gamma'')$ we have $\alpha \times \gamma' = \beta \times \gamma'' = \theta$. We need to prove that $\exists \gamma''' \in \mathcal{A}$ s.t. $\alpha \times \beta \times \gamma''' = \theta = \alpha \times \gamma' = \beta \times \gamma''$ which by the completeness results means that $T = I(\alpha \times \beta \times \gamma''')$.

The interpretation function I is applied to the canonical almost normal form, and therefore we consider the actions $\alpha \times \gamma'$ and $\alpha \times \beta \times \gamma'''$ to be in c.a.n.f.. Because the canonical form is defined inductively it is w.l.o.g. that we look only at the first levels of the actions (i.e. only at the concurrent actions $\alpha_{\times}^{i}$ of the canonical form). For a simple notation we denote the concurrent actions on the first level of α by $\alpha_1, \alpha_2, \ldots, \alpha_k$; note that there are k actions in total. For the action β we denote the concurrent actions on the first level by $\beta_1, \beta_2, \ldots, \beta_l$. For the action θ we denote the concurrent actions by τ_i.

To prove the lamma we use the proof principle *reductio ad absurdum* and suppose that $\alpha \times \beta \times \gamma''' \neq \theta$ is the case. According to the above this supposition is equivalent to saying that the concurrent actions on the first

level of θ are not constructed from the actions on the first level of $\alpha \times \beta$. This may be from several reasons.

First consider that a concurrent action of $\alpha \times \beta$, say $\alpha_1 \times \beta_1$ is not contained in any of the concurrent actions τ_i on the first level of θ. Consider $\tau^i_{\alpha_1}$ to be those τ_i which contain α_1; and similarly consider $\tau^j_{\beta_1}$ those τ_i which contain β_1. From the supposition we know that β_1 does not appear in any of the $\tau^i_{\alpha_1}$; and similarly α_1 does not appear in any $\tau^j_{\beta_1}$. From the hypothesis $\theta = \beta \times \gamma''$ we know that in all τ it appears one of the β_j concurrent actions. This means that in each of the $\tau^i_{\alpha_1}$ it appears one of the β_j where $j \neq 1$. Consider w.l.o.g. one of these actions $\tau^1_{\alpha_1} = \alpha_1 \times \beta_2 \times \gamma$ for some γ which may also be empty. From the same hypothesis $\theta = \beta \times \gamma''$ and knowing that $\alpha_1 \times \beta_2 \times \gamma$ is a concurrent action on the first level of θ then it means that $\alpha_1 \gamma$ is an action on the first level of γ''. This means that between the actions τ of the first level of θ there exists each of the actions $\alpha_1 \times \gamma \times \beta_j$ with $j \neq 2$ (because we allready have the index 2). In other words, the action $\alpha_1 \times \gamma$ must be combined with any of the actions β_j including β_1.

We thus obtained the contradiction (i.e. there exists an action τ which contains $\alpha_1 \times \beta_1$). Therefore, each of the $\alpha_i \times \beta_j$ of $\theta = \alpha \times \beta \times \gamma'''$ are contained in τ_i. In other words we have proven that all the concurrent actions on the first level of the action $\alpha \times \beta$ are found among the concurrent actions on the first level of θ. Moreover, the discussion above also proves that $\forall \tau \in \theta,\ \tau = \alpha_i \beta_j \gamma$; which says that there is no concurrent action on the first level of θ which does not contain an action from the first level of $\alpha \times \beta$.

The only way to stil have the (bad) supposition is to say that it is not the case that for all pairs $\alpha_i \beta_j$ there exits a same γ such that $\alpha_i \times \beta_j \times \gamma = \tau$ is a concurrent action on the first level of θ. To explain it differently, this supposition wants to contradict the second $\times$ operator in the conclusion of the lemma $(\alpha \times \beta) \times \gamma'''$ which by the definition it must be that for each γ an action on the first level of γ''' it must be combined with each action $\alpha_i \times \beta_j$ of $\alpha \times \beta$.

We take an arbitrary pair $\alpha_i \times \beta_j$, say $\alpha_1 \times \beta_1$ and w.l.o.g. suppose it has some extra action $\gamma_\times$ which may be also empty. Thus $\alpha_1 \times \beta_1 \times \gamma_\times$ is an action on the first level of θ. From the hypothesis $\beta \times \gamma'' = \theta$ and knowing that β_1 is combined with the action $\alpha_1 \times \gamma_\times$ it implies that all other β_j with $j \neq 1$ must be combined with the same action. Therefore, the following are also actions τ: $\alpha_1 \times \beta_2 \times \gamma_\times, \ldots, \alpha_1 \times \beta_{n''} \times \gamma_\times$. On the other hand, from the hypothesis $\alpha \times \gamma' = \theta$ and knowing that $\alpha_1 \times \beta_1 \times \gamma_\times$ is a τ action it means that all other α_i actions must be combined with $\beta_1 \times \gamma_\times$. Therefore, we also have as τ actions: $\alpha_2 \times \beta_1 \times \gamma_\times, \ldots, \alpha_k \times \beta_1 \times \gamma_\times$.

We continue to apply recursively the same reasoning on the new deduced actions like $\alpha_2 \times \beta_1 \times \gamma$ and we obtain in the end that all the actions $\alpha_k \times \beta_l$ appear among the actions τ on the first level of θ combined with the same

action $\gamma_\times$. Thus, the second false supposition is contradicted.

The last way of contradicting the lemma is trivial and it supposes that it is not the case that all the τ actions of θ come from combination by $\times$ with the actions $\alpha_i \times \beta_j$. More clearly this tries to say that there exit other τ actions that do not follow the pattern deduced by the first two reasonings we had before. This cannot be as if there were another action besides $\alpha_i \times \beta_j \times \gamma_\times$, say τ' we have proven by contradicting the first supposition that this must be of the form $\alpha_i \times \beta_j \times \gamma'_\times$ and by the second supposition we again get that there exist all the $\alpha_i \times \beta_j \times \gamma'_\times$ as actions τ on the first level of θ.

The proof of the lemma is finished, as the bad supposition is allways contradicted. □

Lemma 3.8 *For any N a normative structure and α, β two distinct actions we have that if $N, i \models O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta)$ then $I(\alpha \times \beta)\ \mathcal{S}_i\ N$.*

Proof: We use Lemma 3.7 and mainly the fairness constraint on obligations from Definition 3.1. The purpose of fair obligations is not necessarily a technical but also a practical one. The fairness constraint refers mainly to choices of actions, as when deciding on which of the actions to choose the model should not influence the decision. For example in the model of Fig. 2(iii) the action $a + b$ is obligatory. Change now this model by adding to the left label a c action and to the right label a d. The action $a + b$ is still obligatory, but when deciding which of a or b to take one needs to take into account the two distinct actions c and d (which one "likes" most). If we were to add the same label c to both branches then the fairness constraint is satisfied, as one does not care about the extra action c when choosing.

From the statement of the lemma $N, i \models O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta)$ by applying the Lemma 3.5 we get that $N_{max}^{I(\alpha),i} = N_{max}^{I(\beta),i}$ (we treat the two cases with strict inclusion at the end). This implies (see Corollary 3.6) that the corresponding trees which unfold these maximal substructures are the same; i.e. $TN_{max}^{I(\alpha),i} = TN_{max}^{I(\beta),i} = TN_{max}$.

Moreover, from the hypothesis of the lemma we get that $N, i \models O_{\mathcal{C}}(\alpha)$ and $N, i \models O_{\mathcal{C}}(\beta)$. Considering the *fair obligations* constraint it implies that:

$$\exists \gamma' \text{ s.t. } I(\alpha \times \gamma') = TN_{max}^{I(\alpha),i}$$
$$\exists \gamma'' \text{ s.t. } I(\beta \times \gamma'') = TN_{max}^{I(\beta),i}$$

From these and knowing that the maximal simulating structures are the same we get that $I(\alpha \times \gamma') = I(\beta \times \gamma'') = TK_{max}$. By applying the Lemma 3.7 we get that $TK_{max} = I(\alpha \times \beta \times \gamma''')$.

Following the Definition 2.10 of the simulation relation $\mathcal{S}_i$, in order to prove the conclusion $I(\alpha \times \beta)\ \mathcal{S}_i\ N$ we need to prove that:

(1) $\forall r \xrightarrow{\gamma} t' \in I(\alpha \times \beta)$, $\exists i \xrightarrow{\gamma'} k' \in N$ s.t. $\gamma \subseteq \gamma'$ and $t' \mathcal{S} k'$,

(2) $\forall i \xrightarrow{\gamma'} k' \in N$ with $\gamma \subseteq \gamma'$ then $t' \mathcal{S} k'$.

Using the results of the previous lemmas the proofs of (1) and (2) become simple. As $I(\alpha \times \beta \times \gamma''') = TN_{max}$ which is the tree unfolding of the substructure $N_{max} = N_{max}^{I(\alpha),i} = N_{max}^{I(\beta),i}$ of N, then it is simple to see that for any edge $r \xrightarrow{\gamma} t' \in I(\alpha \times \beta)$ there is a transition $i \xrightarrow{\gamma'} k' \in TN_{max}$ which clearly $\gamma \subseteq \gamma'$ depending on γ'''. Therefore, $i \xrightarrow{\gamma'} k' \in N_{max}$ and thus $i \xrightarrow{\gamma'} k' \in N$. The fact that $t' \mathcal{S} k'$ is true is obvious by applying a similar recursive reasoning and descending one level in the tree. Note that the recursive reasoning stops when the tree node t' has no more children (i.e. no more edges $t' \xrightarrow{\gamma} t''$ exist in $I(\alpha \times \beta)$); and this is always the case as the tree is finite.

For proving (2) we use a similar recursive reasoning as before. From the condition $\gamma \subseteq \gamma'$ it implies that $\gamma' = \gamma \times \gamma''$. Because γ' is a label of a transition in $I(\alpha \times \beta \times \gamma''')$ then $\gamma' = \alpha \times \beta \times \gamma'''_{\times} \times \gamma''$ which because it contains α it enters under the application of the hypothesis $I(\alpha)\ \mathcal{S}_i\ N$ (and similarly because it contains β we can apply $I(\beta)\ \mathcal{S}_i\ N$). Applying the hypothesis leads to the fact there there are the edges $r \xrightarrow{\gamma} t'_\alpha \in I(\alpha)$ and $r \xrightarrow{\gamma} t'_\beta \in I(\beta)$ with $t'_\alpha \mathcal{S} k'$ and $t'_\beta \mathcal{S} k'$. On the other hand t' comes from the combination of the two t'_α and t'_β and thus a simple recursive reasoning gives $t' \mathcal{S} k'$. The recursive reasoning stops again when the node t' has no more children.

Note that if we consider inclusion among the maximal simulating structures (instead of the equality as we did) then the discussion above does not change. The $TN_{max}^{I(\alpha \times \beta),i}$ is the same as the interpretation $I(\alpha \times \beta \times \gamma''')$. □

Two corollaries of Lemmas 3.5 and 3.8: first shows what is the maximal simulating structure with respect to $I(\alpha \times \beta)$; and the second states that the obligation of $\alpha \times \beta$ respects the fairness contraint. Corollary 3.9 is used in both the proof of Lemma 3.11 and in the proof of the third requirement of the semantics of $O(\alpha \times \beta)$.

Corollary 3.9 *For any N a normative structure and α, β two distinct actions we have that if $N, i \models O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta)$ then either*
$N_{max}^{I(\alpha),i} = N_{max}^{I(\beta),i} = N_{max}^{I(\alpha \times \beta),i}$ *or*
$N_{max}^{I(\alpha),i} \subset N_{max}^{I(\beta),i} = N_{max}^{I(\alpha \times \beta),i}$ *or*
$N_{max}^{I(\beta),i} \subset N_{max}^{I(\alpha),i} = N_{max}^{I(\alpha \times \beta),i}$.

Corollary 3.10 *If $N, i \models O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta)$ then $O(\alpha \times \beta)$ respects the fairness constraint of Definition 3.1.*

Lemma 3.11 *If* $N, i \models O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta)$ *then*
$\forall t \xrightarrow{\gamma} t' \in I(\alpha \times \beta)$ *and* $\forall s \xrightarrow{\gamma'} s' \in N$ *s.t.* $t \mathcal{S} s \wedge \gamma \subseteq \gamma'$ *is the case that* $\forall a \in \mathcal{A}_B$ *if* $a \in \gamma$ *then* $\circ_a \in \varrho(s')$.

Proof: It is simple to see, by looking at Definition 2.11, that all transitions $s \xrightarrow{\gamma'} s'$ mentioned in the lemma make up exactly the maximal simulating structure $N_{max}^{I(\alpha\times\beta),i}$. By Corollary 3.9 this is the same as the maximal simulating structures for $I(\alpha)$ and $I(\beta)$.

To finish the proof we take one arbitrary edge $t \xrightarrow{\alpha_\times \times \beta_\times} t' \in I(\alpha \times \beta)$ and one arbitrary transition $s \xrightarrow{\gamma} s' \in N_{max}^{I(\alpha\times\beta),i}$ s.t. $t \mathcal{S} s$ and $\gamma = \alpha_\times \times \beta_\times \times \gamma'$ where γ' may also be $\mathbf{1}$. These satisfy the conditions in the lemma. The edge $t \xrightarrow{\alpha_\times \times \beta_\times} t'$ comes from the combination of two edges $t \xrightarrow{\alpha_\times} t' \in I(\alpha)$ and $t \xrightarrow{\beta_\times} t' \in I(\beta)$. On the other hand we have for the transition $s \xrightarrow{\gamma} s'$ that both $\alpha_\times \subseteq \gamma$ and $\beta_\times \subseteq \gamma$ hold. This means that we can apply the hypothesis of the lemma (i.e. apply the definition for $O_{\mathcal{C}}$ to both $O_{\mathcal{C}}(\alpha)$ and $O_{\mathcal{C}}(\beta)$) to get that $\circ_a \in \varrho(s'), \forall a \in \alpha_\times$ and $\circ_a \in \varrho(s'), \forall a \in \beta_\times$ (because the definition says that for all transitions this happens). This implies the result of the lemma, i.e. $\circ_a \in \varrho(s'), \forall a \in \alpha_\times \times \beta_\times$. □

Lemma 3.12 *If* $N, i \models O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta)$ *then*
$N, s \models \mathcal{C} \quad \forall s \in N$ *with* $t \hat{\mathcal{S}} s \wedge t \in$ *leafs*$(I(\overline{\alpha \times \beta}))$.

Proof : The conclusion of the lemma should be read as: the formula $\mathcal{C}$ holds in all those states $s \in N$ which can be reached by "following" the tree interpretation of the action negation $\overline{\alpha \times \beta}$ to the leafs. By "to follow" we mean that the normative structure simulates *strictly* the tree $I(\overline{\alpha \times \beta})$. The simulation must be strict so that we follow *exactly* the tree.

Recall the Definition 2.5 of the action negation. The negation of a compound action $\overline{\alpha}$ works on each level of the negated action α. For the proof of this lemma it is enough to look at the behavior for only the first level, and for the rest we apply a similar recursive reasoning. Moreover, note that we need to look only at the leafs of the trees (i.e. at the states from the end of the full paths of the tree interpretation of the negated action). Thus, the first level in the negation contains the choice $+_{\gamma \in \overline{R}} \gamma$ (defining the full branches; we look at the other full branches when we reason recursively at lower levels of the tree).

Thus, we need to prove that $\forall t \xrightarrow{\gamma} t' \in I(+_{\gamma \in \overline{R}} \gamma)$ with $\gamma \in \mathcal{A}_B^\times$ a concurrent action s.t. $\forall \alpha_\times^i \times \beta_\times^j$ a concurrent action on the first level of the tree of the negated action $\alpha \times \beta$ we have that $\alpha_\times^i \times \beta_\times^j \not\subseteq \gamma$ then it is the case that if $\exists s \xrightarrow{\gamma} s' \in N$ then $N, s' \models \mathcal{C}$. Take an arbitrary transition $t \xrightarrow{\gamma} t'$

for which the above hold and for which $\exists s \xrightarrow{\gamma} s' \in N$ and we show that $N, s' \models \mathcal{C}$.

From the condition $\forall \alpha_\times^i \times \beta_\times^j, \alpha_\times^i \times \beta_\times^j \not\subseteq \gamma$ we can conclude that either $\forall \alpha_\times^i, \alpha_\times^i \not\subseteq \gamma$ or $\forall \beta_\times^j, \beta_\times^j \not\subseteq \gamma$. This is done by using the proof principle *reductio ad absurdum* and we suppose that neither of the $\forall \alpha_\times^i, \alpha_\times^i \not\subseteq \gamma$ nor $\forall \beta_\times^j, \beta_\times^j \not\subseteq \gamma$ hold. This means that $\exists i', j'$ s.t. $\alpha_\times^{i'} \subseteq \gamma \wedge \beta_\times^{j'} \subseteq \gamma$ which implies that $\alpha_\times^{i'} \times \beta_\times^{j'} \subseteq \gamma$. By looking again at the definition of the $\times$ operation we see that $\alpha_\times^{i'} \times \beta_\times^{j'}$ must be an action among the $\alpha_\times^i \times \beta_\times^j$. Therefore, the conclusion that we have just drawn before enters into contradiction with the initial condition $\forall \alpha_\times^i \times \beta_\times^j, \alpha_\times^i \times \beta_\times^j \not\subseteq \gamma$.

By using one of the hypothesis of the lemma, say $N, i \models O_{\mathcal{C}}(\alpha)$ we conclude from the definition of the semantics of $O_{\mathcal{C}}$ that the transition that we work with $t \xrightarrow{\gamma} t'$ respects the fact that $\forall \alpha_\times^i, \alpha_\times^i \not\subseteq \gamma$ and thus in the end state of the stransition $s \xrightarrow{\gamma} s' \in N$ we have $N, s' \models \mathcal{C}$. This is the conclusion of the lemma. □

Proof of Theorem 3.4: We need to prove that $N, i \models O_{\mathcal{C}}(\alpha \times \beta)$ under the assumption $N, i \models O_{\mathcal{C}}(\alpha) \wedge O_{\mathcal{C}}(\beta)$. Using the Lemma 3.8 we have that $I(\alpha \times \beta)\ \mathcal{S}_i\ N$ which is the first requirement in the semantics of $O_{\mathcal{C}}$. From Lemma 3.11 we get that $\forall t \xrightarrow{\gamma} t' \in I(\alpha \times \beta)$ and $\forall s \xrightarrow{\gamma'} s' \in N$ s.t. $t\, \mathcal{S}\, s \wedge \gamma \subseteq \gamma'$ then $\forall a \in \mathcal{A}_B$ if $a \in \gamma$ then $\circ_a \in \varrho(s')$ which is the second requirement. The last requirement is proven in the Lemma 3.12.

We remain to prove the third requirement which states that $\forall s \xrightarrow{\gamma'} s' \in N_{rem}^{I(\alpha \times \beta), i}$ then $\forall a \in \mathcal{A}_B$ if $a \in \gamma'$ then $\circ_a \notin \varrho(s')$. Following from Corollary 3.9 is that $N_{rem}^{I(\alpha \times \beta), i} = N_{rem}^{I(\alpha), i} = N_{rem}^{I(\beta), i}$ (the cases for inclusion are treated at the end). From the hypothesis $N, i \models O_{\mathcal{C}}(\alpha)$ we have that $\forall s \xrightarrow{\gamma'} s' \in N_{rem}^{I(\alpha), i}$ then $\forall a \in \mathcal{A}_B$ if $a \in \gamma'$ then $\circ_a \notin \varrho(s')$ which makes our proof goal also true by replacing $N_{rem}^{I(\alpha), i}$ with its equal $N_{rem}^{I(\alpha \times \beta), i}$.

In the case when $N_{max}^{I(\alpha), i} \subset N_{max}^{I(\beta), i} = N_{max}^{I(\alpha \times \beta), i}$ then we work as before but consider the structure for β instead.

The proof of the main result is finished. □

Corollary 3.13 $\models O_{\mathcal{C}_1}(\alpha) \wedge O_{\mathcal{C}_2}(\beta) \rightarrow O_{\mathcal{C}_1 \vee \mathcal{C}_2}(\alpha \times \beta)$.

The following result shows that the semantics avoids several *unwanted implications*.

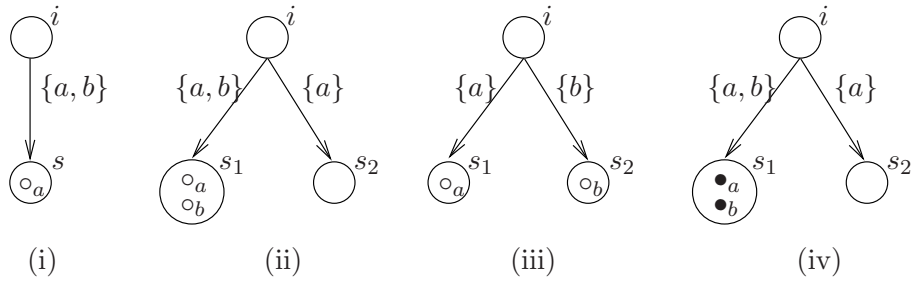

Figure 2: Counterexamples for Proposition 3.14.

Proposition 3.14 *The following statements are true:*

$$\not\models O_{\mathcal{C}}(\alpha) \rightarrow O_{\mathcal{C}}(\alpha \times \beta); \tag{11}$$
$$\not\models O_{\mathcal{C}}(\alpha \times \beta) \rightarrow O_{\mathcal{C}}(\alpha); \tag{12}$$
$$\not\models O_{\mathcal{C}}(\alpha + \beta) \rightarrow O_{\mathcal{C}}(\alpha \times \beta); \tag{13}$$
$$\not\models O_{\mathcal{C}}(\alpha \times \beta) \rightarrow O_{\mathcal{C}}(\alpha + \beta); \tag{14}$$
$$\not\models O_{\mathcal{C}}(\alpha) \rightarrow O_{\mathcal{C}}(\alpha + \beta); \tag{15}$$
$$\not\models O_{\mathcal{C}}(\alpha + \beta) \rightarrow O_{\mathcal{C}}(\alpha). \tag{16}$$

Proof sketch: The proof is simple by giving for each statement a counterexample. In Fig. 2(i) we have a model for which $O_{\mathcal{C}}(a)$ holds in state i but $O_{\mathcal{C}}(a \times b)$ does not hold (i.e. first statement) and also $O_{\mathcal{C}}(a + b)$ does not hold (i.e. fifth statement). In the model of Fig. 2(ii) $O_{\mathcal{C}}(a \times b)$ holds in state i but $O_{\mathcal{C}}(a)$ does not hold (i.e. second statement) and also $O_{\mathcal{C}}(a + b)$ does not hold (i.e. forth statement). In the last model of Fig. 2(iii) $O_{\mathcal{C}}(a + b)$ holds in state i but $O_{\mathcal{C}}(a \times b)$ does not hold (i.e. third statement) and also $O_{\mathcal{C}}(a)$ does not hold (i.e. sixth statement). □

Proposition 3.15 *The following statements are true:*

$$\models F_{\mathcal{C}}(\alpha) \rightarrow F_{\mathcal{C}}(\alpha \times \beta) \tag{17}$$
$$\models F_{\mathcal{C}}(\alpha + \beta) \leftrightarrow F_{\mathcal{C}}(\alpha) \wedge F_{\mathcal{C}}(\beta) \tag{18}$$
$$\models P(\alpha + \beta) \leftrightarrow P(\alpha) \wedge P(\beta) \tag{19}$$
$$\not\models F_{\mathcal{C}}(\alpha \times \beta) \rightarrow F_{\mathcal{C}}(\alpha) \tag{20}$$
$$\not\models P(\alpha \times \beta) \rightarrow P(\alpha) \tag{21}$$

Proof: We give first quick proof arguments. The proof of the first statement (17) is based on the fact that paths in $I(\alpha \times \beta)$ contain (i.e. have larger labels) than paths of $I(\alpha)$. Based on, it is simple to find a counterexample example to prove the forth statement (20): in Fig. 2(iv) the model makes $F_{\mathcal{C}}(a \times b)$

true and $F_{\mathcal{C}}(a)$ false. The proof of the second statement (18) is based on the fact the the paths of $I(\alpha+\beta)$ which satisfy the condition in the semantics are the same as the paths of $I(\alpha)$ and $I(\beta)$ together.

For the proof of $\models F_{\mathcal{C}}(\alpha) \rightarrow F_{\mathcal{C}}(\alpha \times \beta)$ consider an arbitrary pointed structure N, i which makes $F_{\mathcal{C}}(\alpha)$ true. In order to show that $N, i \models F_{\mathcal{C}}(\alpha \times \beta)$ we need to take an arbitrary full path $\sigma \in I(\alpha \times \beta)$ which satisfies $\sigma \, \mathcal{S}_i \, N$ and we need to find an edge $t \xrightarrow{\gamma} t'$ on this path for which the condition in the semantics is satisfied: $\forall s \xrightarrow{\gamma'} s' \in N$ with $t \, \mathcal{S} \, s \wedge \gamma \subseteq \gamma'$ then $\forall a \in \mathcal{A}_B$ if $a \in \gamma'$ then $\bullet_a \in \varrho(s')$. Note that if a path $\sigma \in I(\alpha \times \beta)$ exists then it exists also a path $\sigma' \in I(\alpha)$ which has all the labels on the edges smaller than the corresponding ones in σ. Therefore this is also a path which satisfies $\sigma' \, \mathcal{S}_i \, N$. We can apply the semantics for the expression $F_{\mathcal{C}}(\alpha)$ to deduce that there is an edge $t \xrightarrow{\gamma} t' \in \sigma'$ for which all transitions $s \xrightarrow{\gamma'} s' \in N$ satisfying $\gamma \subseteq \gamma'$ also satisfy $\forall a \in \mathcal{A}_B$ if $a \in \gamma'$ then $\bullet_a \in \varrho(s')$. We can find now a corresponding edge in σ which has a label γ'' which includes γ. Therefore, from all the transitions $s \xrightarrow{\gamma'} s'$ before we need to look only at some of them which respect $\gamma'' \subseteq \gamma'$. But all these transitions we know that respect $\forall a \in \mathcal{A}_B$ if $a \in \gamma'$ then $\bullet_a \in \varrho(s')$. Therefore proof is finished.

It should be simple to see that the opposite implication does not allways hold; i.e. $\not\models F_{\mathcal{C}}(\alpha \times \beta) \rightarrow F_{\mathcal{C}}(\alpha)$. This is because we cannot guarantee that by taking all the paths $\sigma' \in I(\alpha \times \beta)$ which satisfy $\sigma' \, \mathcal{S}_i \, N$ we will consider all the paths $\sigma \in I(\alpha)$, because there may be paths with labels smaller that those in $I(\alpha \times \beta)$ which are still good paths for $I(\alpha)$. Take the example in Fig. which is a model for $F_{\mathcal{C}}(a \times b)$ but is not a model for $F_{\mathcal{C}}(a)$.

The proof for $\models F_{\mathcal{C}}(\alpha+\beta) \leftrightarrow F_{\mathcal{C}}(\alpha) \wedge F_{\mathcal{C}}(\beta)$ is more simple. It is easy to see that the tree $I(\alpha+\beta)$ contains all the full paths σ of the two trees $I(\alpha)$ and $I(\beta)$ which satisfy $\sigma \, \mathcal{S}_i \, N$. Therefore, the double implication is immediate as if we consider $F_{\mathcal{C}}(\alpha+\beta)$ true than the traces in $I(\alpha+\beta)$ respect all the conditions of the semantics and thus all the traces in $I(\alpha)$ respect the conditions in the semantics, making $F_{\mathcal{C}}(\alpha)$ true (and the same for $F_{\mathcal{C}}(\beta)$).

The proof of (19) is similar to the proof of (18) from above.

For the proof of $\not\models P(\alpha \times \beta) \rightarrow P(\alpha)$ take the structure in Fig. 2 and add a marker $\bullet_a$ to state s_2. This is a model for $P(\alpha \times \beta)$ but obviously is not a model for $P(\alpha)$. □

Proposition 3.16 (paradoxes) *The following paradoxes*[4] *are avoided:*

- *Ross's paradox*
- *The Free Choice Permission paradox*

[4]See [McN06] for a description of each paradox.

- *Sartre's dilemma*
- *The Good Samaritan paradox*
- *The Gentle Murderer paradox*

Proof : In short, Ross's paradox is avoided because of using obligations over actions and not over propositions. Sartre's dilemma is ruled out by either the third statement of Proposition 3.1 or by using conflicting actions. The good Samaritan paradox is ruled out by our ought-to-do approach and it becomes just a conditional obligation. □

4 Properties of the Logic

The following help in proving a *tree model property.*

Definition 4.1 *A* tree structure*, denoted by* $TN, \varepsilon = (\mathcal{W}^T, R^T_{2^{\mathcal{A}_B}}, \mathcal{V}^T, \varrho^T)$*, is a pointed normative structure* N, s *which has the shape of a tree as in Definition 2.7; i.e. it respects the following restrictions:*

- *name the nodes with strings of natural numbers* $\mathcal{W}^T \subset \mathbb{N}^*$ *s.t.* $s = \varepsilon$*;*
- *for each label* $\alpha \in 2^{\mathcal{A}_B}$ *the partial function* $R^T_{2^{\mathcal{A}_B}}(\alpha) : \mathcal{W}^T \to \mathcal{W}^T$ *respects the restriction:* $R^T_{2^{\mathcal{A}_B}}(\alpha)(x) = xi$ *where* $x, xi \in \mathcal{W}^T$ *and* $i \in \mathbb{N}$*;*
- *for any* $\alpha \neq \beta \in 2^{\mathcal{A}_B}$ *then* $R^T_{2^{\mathcal{A}_B}}(\alpha)(x) \neq R^T_{2^{\mathcal{A}_B}}(\beta)(x)$ *for any* $x \in \mathcal{W}^T$*.*

Lemma 4.1 (tree model) *Given a pointed normative structure* N, i *then we can construct an associated tree structure* TN, ε*.*

Proof: The technique that we use is known in modal logics as the tree unfolding of a Kripke structure [Sah75,HKT00]. For a pointed normative structure $N, i = (\mathcal{W}, R_{2^{\mathcal{A}_B}}, \mathcal{V}, \varrho)$ we can view the set of worlds $\mathcal{W} = \{0, 1, 2, \dots\}$ to be the natural numbers $\mathbb{N}$; and we define the set $\mathcal{W}^T[i] \subset \mathbb{N}^*$ to be the set of finite paths starting from i. Moreover, we want to enrich the paths to contain also the labels by which the path was formed. For this we interplace between the nodes labels from $2^{\mathcal{A}_B}$. That is, i is considered the empty set ε, the paths of depth one are $\varepsilon\alpha s \mid s \in \mathcal{W}$ s.t. $i \xrightarrow{\alpha} s$ is a transition in N. We define a function $\rho : \mathcal{W}^T[i] \to \mathcal{W}$ which assigns to each path the state in which the path ends; e.g. $\rho(\varepsilon\alpha s'\beta s'') = s''$. Note that two paths $x\alpha s$ and $x\beta s$ are regarded as different. Consider the set $\mathcal{W}[i] = \{\rho(x) \mid x \in \mathcal{W}^T[i]\}$ of states reachable (by any path) from the node i. The function $\rho : \mathcal{W}^T[i] \to \mathcal{W}[i]$ is a surjection therefore it exists the corresponding function ρ^{-1} which returns sets of traces from $\mathcal{W}^T[i]$.

For the pointed structure N, i we construct the pointed structure $TN, \varepsilon = (\mathcal{W}^T[i], R^T_{2^{\mathcal{A}_B}}, \mathcal{V}^T, \varrho^T)$. The function $R^T_{2^{\mathcal{A}_B}}$ assigns to each α a partial function $R^T_{2^{\mathcal{A}_B}}(\alpha) : \mathcal{W}^T[i] \to \mathcal{W}^T[i]$ (we write the partial functions as sets of pairs of argument/value) which is defined as:

$$R^T_{2^{\mathcal{A}_B}}(\alpha) = \{(x, x\alpha s) \mid (\rho(x), s) \in R_{2^{\mathcal{A}_B}}(\alpha)\}.$$

The valuation function $\mathcal{V}^T$ is defined in terms of $\mathcal{V}$:

$$\mathcal{V}^T(\phi) = \rho^{-1}(\mathcal{V}(\phi)).$$

The above notation is standard and is using a set of elements as argument of the function ρ^{-1} and returns the corresponding set of values (by doing the union of the sets of traces). The marking function ϱ^T is defined in terms of ϱ:

$$\varrho^T(x) = \varrho(\rho(x)).$$

It is easy to see that TN, ε is a tree structure with root node ε. We can check that TN, ε is a normative structure. The restrictions imposed by the tree structure definition on the function $R^T_{2^{\mathcal{A}_B}}$ are met. By construction, for any of the partial functions $R^T_{2^{\mathcal{A}_B}}(\alpha)$ it cannot be the case that $R^T_{2^{\mathcal{A}_B}}(\alpha)(x) = y\alpha s$ where $x \neq y$ (i.e. the first restriction is met). Take now two different actions $\alpha \neq \beta$ then it cannot be the case that $R^T_{2^{\mathcal{A}_B}}(\alpha)(x) = R^T_{2^{\mathcal{A}_B}}(\beta)(x)$ because $R^T_{2^{\mathcal{A}_B}}(\alpha)(x) = x\alpha s \neq x\beta s' = R^T_{2^{\mathcal{A}_B}}(\beta)(x)$ even if $s = s'$. □

Theorem 4.2 *For a pointed structure N, i we have:*

$$TN, x \models \mathcal{C} \quad \textit{iff} \quad N, \rho(x) \models \mathcal{C} \tag{22}$$

$$TN, \varepsilon \models \mathcal{C} \quad \textit{iff} \quad N, i \models \mathcal{C} \tag{23}$$

Proof sketch: The proof of (23) follows from (22) by replacing x with ε (and thus $\rho(\varepsilon) = i$). The proof of (22) is done by induction on the structure of the formula $\mathcal{C}$. It has lengthy but easy cases as it needs to prove each of the conditions in the definitions of the semantics of the deontic modalities. □

Corollary 4.3 (tree model property) *If a formula $\mathcal{C}$ has a model N then it has a tree model TN.*

Proof : This follows immediately from equation (23) of the Theorem 4.2 which says that if a formula $\mathcal{C}$ is true in a state i of a model N then there

exists a model TN in which the formula is true in state ε. By the Lemma 4.1 this pointed structure TN, ε is a tree. □

Next we prove that the logic has the *finite model property*. Note first that it is rather hard to use the filtration technique in our case. Allready in PDL it was needed the clever idea in the Fischer-Ladner closure which was giving the subformulas of the formula in question. The Fischer-Ladner closure was needed as to know what are the subformulas of a dynamic modality with a complex action inside (e.g. $[a \cdot (b+c)]\phi$). In our case we do not know what are subformulas of an obligation of a complex action like $O_{\mathcal{C}}(a \cdot (b+c))$. We will use the *selection* technique for proving the finite model property [BdRV01, sec.2.3].

Definition 4.2 (action length) *The* length of an action α *is defined (inductively) as a function* $l : \mathcal{A} \to \mathbb{N}$ *from actions to natural numbers.*

- $l(\mathbf{1}) = l(\mathbf{0}) = 0$,
- $l(a) = 1$ *for any basic action* a *of* $\mathcal{A}_B$,
- $l(\alpha \& \beta) = l(\alpha + \beta) = max(l(\alpha), l(\beta))$,
- $l(\alpha \cdot \beta) = l(\alpha) + l(\beta)$.

The length function counts the number of actions in a sequence of actions given by the $\cdot$ constructor. We say that $\alpha(n)$ identifies the action of length $0 < n \leq l(\alpha)$ in the action α. For $n = 0$, $\alpha(0) = \mathbf{1}$ returns the implicit *skip* action, which is natural because every action α can have as starting action $\mathbf{1}$, i.e. $\alpha = \mathbf{1} \cdot \alpha$. For example, for action $\alpha = (a + b) \cdot \mathbf{1} \cdot c$ we have $l(\alpha) = 2$, $\alpha(1) = a + b$ and $\alpha(2) = c$. Note that $\alpha(\cdot)$ ignores $\mathbf{1}$'s.

Proposition 4.4 *For any action* α *we have* $l(\overline{\alpha}) \leq l(\alpha)$.

Proof: First, carefully inspect the Definition 2.5 of action negation. It is easy to see that $\overline{\alpha}$ does not add $\cdot$ combinators at bigger depth than those in α. The negation operation is applied recursively and at each recursive step it generates paths of length 1 for paths of length 1 or greater in the original action α; or it generates paths of length 1+ length generated in the next recursive step. This happens for each $\cdot$ found in α. Therefore, $\overline{\alpha}$ cannot have paths of greater depth than the paths in α □

Corollary 4.5 *For any action* α *we have* $h(I(\overline{\alpha})) \leq h(I(\alpha)) = l(\alpha)$.

Proof: This is a corollary of both Theorem 2.8 and Proposition 4.4. □

Definition 4.3 (nesting degree) *We define the* degree *of a formula inductively as a function d from formulas to natural numbers:*

- $d(\phi) = d(\bot) = 0$*;*
- $d(\mathcal{C}_1 \rightarrow \mathcal{C}_2) = max(d(\mathcal{C}_1), d(\mathcal{C}_2))$*;*
- $d(O_{\mathcal{C}}(\alpha)) = d(F_{\mathcal{C}}(\alpha)) = 1 + d(\mathcal{C})$*;*
- $d(P(\alpha)) = 1$.

We give two definitions of *depth* of a formula; one is a more raw approximation and the second is a more fidel approximation of the real depth. The depth of a formula gives the maximum number of transitions (in a chain) that one needs to inspect in a model in order to know the truth value of the formula.

Definition 4.4 (depth of formula) *We define the* raw depth *of a formula $\mathcal{C}$ to be $d(\mathcal{C}) * max(l(\alpha) \mid \forall \alpha \in \mathcal{C})$; which multiplies the degree of the formula with the maximal length of the actions that appear in the formula (at any degree). We define the* fidel depth *to be sum of the lengths of all the actions of the formula. Note that there is one action per degree level.*

It is simpler to work with the raw depth so we use that in the following.

Lemma 4.6 *Take a formula $\mathcal{C}$ with raw depth k. If $TN, \varepsilon \models \mathcal{C}$ then $\mathcal{C}$ holds in the root of the tree structure TN, ε restricted to paths of maximum depth k (i.e. where all nodes of depth $> k$ are removed).*

Proof: The proof for formulas $\bot$ and ϕ which have raw depth 0 is simple as by the semantics we need to inspect only the root node ε therefore we need only nodes of depth 0 in the tree structure.

For the formula $P(\alpha)$ which has raw depth $1 * l(\alpha)$ we need to inspect only those states of TN, ε which respect the simulation relation. Therefore, the maximum depth of a state is the maximum length in the final paths in $I(\alpha)$, amd thus the maximum depth of the nodes in tN, ε is $l(\alpha)$.

For the formula $\mathcal{C}_1 \rightarrow \mathcal{C}_2$ we use structureal induction. The basis case was proven in the first two paragraphs. Now the raw depth of the formula is the maximum of the raw depth of the two subformulas; w.l.o.g. say the raw depth of $\mathcal{C}_1$. From the semantics we know that we need to check to see if $\mathcal{C}_1$ holds which the inductive hypothesis we need a tree of depth at most the raw degree of $\mathcal{C}_1$. If $\mathcal{C}_1$ holds we need to check also $\mathcal{C}_2$ which requires also a tree of depth at most the raw degree of $\mathcal{C}_2$. Therefore, overall we need to check a tree with at most depth the raw degree of $\mathcal{C}_1$.

The proof for the formulas $O_{\mathcal{C}}(\alpha)$ and $F_{\mathcal{C}}(\alpha)$ is similar and we do the proof only for obligations. We use induction on the nesting degree of the

modality. The base case is when the $\mathcal{C} \in \{\bot, \phi\}$ is of nesting degree 0 and thus $O_{\mathcal{C}}(\alpha)$ is of nesting degree 1. The semantics of $O_{\mathcal{C}}$ says that we need to check first the obligation alone which requires nodes of depth at most the length of α because of the simulation relation. Secondly we need to check that the reparation $\mathcal{C}$ holds at the states corresponding to the leaf nodes of the negation $\overline{\alpha}$. By Corollary 4.5 we know that these states are at depth at most $l(\alpha)$ and from the first two paragraphs we know that testing $\bot$ or ϕ does not require deeper nodes. Thus, because $l(\alpha) \leq max(l(\alpha') \mid \forall \alpha' \in O_{\mathcal{C}}(\alpha'))$ the base case is proven to require trees with depth at most the raw degree of the formula.

The inductive case supposes that to check $\mathcal{C}$ it is required a tree of depth at most the raw degree $d(\mathcal{C}) * max(l(\alpha') \mid \forall \alpha' \in \mathcal{C})$. We need to prove that checking $O_{\mathcal{C}}(\alpha)$ requires a tree with depth at most $(d(\mathcal{C}) + 1) * max(l(\alpha') \mid \forall \alpha' \in O_{\mathcal{C}}(\alpha))$. The discussion is similar to the one before; to check $O_{\mathcal{C}}(\alpha)$ it requires depth at most $l(\alpha)$ and further more we need to check $\mathcal{C}$ starting at a depth of at most $l(\alpha)$. By the induction hypothesis it is required a tree of depth at most $l(\alpha) + d(\mathcal{C}) * max(l(\alpha') \mid \forall \alpha' \in \mathcal{C})$. This number is clearly less than $(d(\mathcal{C}) + 1) * max(l(\alpha') \mid \forall \alpha' \in O_{\mathcal{C}}(\alpha))$ (even when $l(\alpha)$ is greater than $l(\alpha')$ of the other actions). □

Theorem 4.7 (finite model property) *If a formula has a model then it has a finite model.*

Proof: We can work equivalently in pointed structures and then we need to prove that if a formula is satisfied in a pointed structure then it is satisfied in a finite pointed structure. Take a formula $\mathcal{C}$ of raw dept k which is satisfiable in the pointed structure N, i. By Corollary 4.3 we know that $\mathcal{C}$ is satisfied in the tree-like pointed structure TN, ε. Note that the tree might be both infinitely deep and infinitely branching.

By Lemma 4.6 we put a bound on the depth of the tree which is related to the formula. Because we work with deterministic structures and because the set of labels $2^{\mathcal{A}_B}$ is finite as $\mathcal{A}_B$ is finite we have a guaranteed finite branching. Therefore the model is finite. In order to put a fixed bound (related to the formula we check) on the branching of the tree we must cut away all branches that are not needed for checking the formula, and we keep only those that we need (and this should be finitely bounded). □

Theorem 4.8 (decidability)

1. *The logic with general obligations as in the semantic Definition 2.12 is decidable.*
2. *The logic with fair obligations is decidable iff the fairness constraint is decidable.*

5 Conclusion

We have presented a model theoretic semantics based on normative structures for the three deontic operators (obligation, permission, and prohibition) which are applied only over actions. The particularities of the semantics are due to the natural properties that we enforce on the deontic modalities. The most important property relates conjunction of obligations and obligation over synchronous actions. This has not been achieved in the other works that we have mentioned in the introduction. Even more, synchronous actions have not yet been carefully considered under the deontic modalities. Intersection of actions is used in [Mey88, Bro03] to model concurrent actions but in these settings the deontic modalities are encoded in PDL$^{\cap}$ which if interpreted over deterministic structures is known to be undecidable. The definition of action negation as we have it is novel. It formalizes what it means to not performe a (concurrent) action in an eager system (where idling is not possible).

5.1 Open Problems

1. How is the theory changing if we lift the restriction on $\mathcal{A}_B$ and make it a possible infinite set?

References

[BAHP81] Mordechai Ben-Ari, Joseph Y. Halpern, and Amir Pnueli. Finite models for deterministic propositional dynamic logic. In Shimon Even and Oded Kariv, editors, *8th Colloquium On Automata, Languages and Programming (ICALP'81)*, volume 115 of *Lecture Notes in Computer Science*, pages 249–263. Springer, 1981.

[BdRV01] Patrick Blackburn, Maarten de Rijke, and Yde Venema. *Modal Logic*, volume 53 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge Univ. Press, 2001.

[Ber00] Gérard Berry. The foundations of Esterel. In *Proof, language, and interaction: essays in honour of Robin Milner*, pages 425–454. MIT Press, 2000.

[BG92] Gérard Berry and Georges Gonthier. The Esterel synchronous programming language: Design, semantics, implementation. *Sci. Comput. Program.*, 19(2):87–152, 1992.

[BN98] Frantz Baader and Tobias Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.

[Bro03] Jan Broersen. *Modal Action Logics for Reasoning About Reactive Systems.* PhD thesis, Vrije Universiteit Amsterdam, 2003.

[BWM01] Jan Broersen, Roel Wieringa, and John-Jules Ch. Meyer. A fixed-point characterization of a deontic logic of regular action. *Fundam. Inf.*, 48(2-3):107–128, 2001.

[CM] Pablo F. Castro and T.S.E. Maibaum. A complete and compact propositional deontic logic. In Cliff B. Jones, Zhiming Liu, and Jim Woodcock, editors, *4th International Colloquium on Theoretical Aspects of Computing (ICTAC'07)*, volume 4711 of *Lecture Notes in Computer Science*, pages 109–123. Springer-Verlag.

[FL77] Michael J. Fischer and Richard E. Ladner. Propositional modal logic of programs. In *9th ACM Symposium on Theory of Computing (STOC'77)*, pages 286–294. ACM, 1977.

[HKT00] David Harel, Dexter Kozen, and Jerzy Tiuryn. *Dynamic Logic.* MIT Press, 2000.

[Hoa85] C. A. R. Hoare. *Communicating Sequential Processes.* Prentice Hall, 1985.

[LW04] Carsten Lutz and Dirk Walther. PDL with negation of atomic programs. In David A. Basin and Michaël Rusinowitch, editors, *2nd International Joint Conference on Automated Reasoning (IJCAR'04)*, volume 3097 of *Lecture Notes in Computer Science*, pages 259–273. Springer, 2004.

[McN06] Paul McNamara. Deontic logic. In Dov M. Gabbay and John Woods, editors, *Handbook of the History of Logic*, volume 7, pages 197–289. North-Holland Publishing, 2006.

[Mey88] John-Jules Ch. Meyer. A different approach to deontic logic: Deontic logic viewed as a variant of dynamic logic. *Notre Dame Journal of Formal Logic*, 29(1):109–136, 1988.

[Mil83] Robin Milner. Calculi for synchrony and asynchrony. *Theoretical Computer Science*, 25:267–310, 1983.

[Mil95] Robin Milner. *Communication and concurrency*. Prentice Hall, 1995.

[Pra76] Vaughan R. Pratt. Semantical considerations on floyd-hoare logic. In *IEEE Symposium On Foundations of Computer Science (FOCS'76)*, pages 109–121, 1976.

[Pra79] Vaughan R. Pratt. Process logic. In *6th Symposium on Principles of Programming Languages (POPL'79)*, pages 93–100. ACM, 1979.

[Pri08a] Cristian Prisacariu. Extending kleene algebra with synchrony – technicalities. Technical Report 376, Dept. Informatics, Univ. Oslo, Oslo, Norway, October 2008.

[Pri08b] Cristian Prisacariu. A particular matching problem. Technical report, Dept. Informatics, Univ. Oslo, Norway, 2008. (to appear).

[Sah75] Henrik Sahlqvist. Correspondence and completeness in the first- and second-order semantics for modal logic. In Stig Kanger, editor, *Proceedings of the Third Scandanavian Logic Symposium*, pages 110–143. North Holland, Amsterdam, 1975.

[Seg82] Krister Segerberg. A deontic logic of action. *Studia Logica*, 41(2):269–282, 1982.

[Seg92] Krister Segerberg. Getting started: Beginnings in the logic of action. *Studia Logica*, 51(3/4):347–378, 1992.

[vdM96] Ron van der Meyden. The dynamic logic of permission. *Journal of Logic and Computation*, 6(3):465–479, 1996.

[VW68] Georg Henrik Von Wright. *An Essay in Deontic Logic and the General Theory of Action.* North Holland Publishing Co., Amsterdam, 1968.