Multi-level permission

L. Csirmaz[*]

Abstract

Reasoning about permissions and obligations sometimes requires to distinguish more than one level of permission: certain actions are preferable to others, or one has more confidence in one type of action achieving the same goal than in other. We give a logic handling this type of ramification, and present a complete axiomatization. The recent work offers an extension of the *Dynamic Logic of Permission* defined by Meyden [3], where a two-level system was presented. We also prove a separation theorem for the multi-level permission formulas.

1 Introduction

Actions in Dynamic Logic form a free algebra over a (finite) set of *atomic actions*, using the operations ; (composition) $\cup$ (union), and $*$ (iteration). Performing an action transforms a possible state of discourse into another one (thus models of Dynamic Logic are Kripke-style models). Performing $\alpha\,;\beta$ means do (an instance of) α first, and the do (an instance of) β. Doing $\alpha\cup\beta$ means do either α or β. Doing α^* means execute α finitely many (maybe zero) times at your wish. Enhancements of Propositional Dynamic Logic differ in the *modalities* they use. One of the possible approach to describe deontic constructs is dividing the actions into two groups: those which are permitted (or preferable over the others), and those which are possible (but maybe undesirable). In general, we have the modality $\langle\alpha\rangle X$ with the meaning "there exists an execution of α which leads to a state in which X is true" and $\langle\alpha\rangle^* X$ saying that "there is a *permitted* execution of α leading to a state in which X is true." Now suppose one of the realizations of α is "mail the letter," and one β's is "destroy the letter." Then $\langle\alpha\rangle^*\mathbf{true}$ says that it is permitted to mail the letter; $\langle\beta\rangle^*\mathbf{true}$ says that destroying the letter is permitted. In Dynamic Logic the standard semantics for $\langle\alpha\cup\beta\rangle X$ is $\langle\alpha\rangle X\vee\langle\beta\rangle X$. Applying the same semantics to $\langle\alpha\cup\beta\rangle^*$ yields that having permission to mail the letter grants permission immediately to "mail it or destroy it." The standard semantics corresponds to the *not forbidden*, rather than the intuitively more appealing *free choice* permission.

Many ramifications of Dynamic Logic attempts to describe the *free choice* construct of Deontic Logic more adequately, see McCarty [2], Meyden [3], Meyer [4]. In [3] the *Dynamic Logic of Permission* is introduced, and a complete axiomatization is given. The main novelty there is introducing a new modality denoted by $\pi(\alpha, X)$, expressing, loosely speaking, that if α leads to a state where X is true, then all possible executions of α are permitted. This way the free choice is modeled more closely, for example, $\pi(\alpha\cup\beta, X)$ holds if both $\pi(\alpha, X)$ and $\pi(\beta, X)$ are true.

This paper is, in fact, an extension of Meyden's. We assign "confidence" to actions saying how much they are trusted (or permitted), and keep the *not forbidden* and *free choice* modalities enhanced with confidence thresholds. This makes possible to give a more general, but unified treatment of the same subject.

Section 2 describes the syntax and semantics of the multi-level permission logic, and the appropriate axiomatization is given in Section 3, which is proven to be complete in Section 4. As a consequence of our proof, a separation principle is stated and proved in the last section.

[*] Partially supported by DIMACS

2 Syntax and semantics

The *confidence* we assign to elementary actions can be though as percentages: the higher the number the more confident we are in the correctness (or appropriateness) of the given action. They can also be though as abstract entities forming an ordered set, so we can say that we are more confident in one action than in the other. The confidence of a sequence of actions is, evidently, the confidence of its weakest element, i.e., their minimum. However, when the confidence of a *set* of action sequences should be determined, we have two obvious choice. First, if some sequence in the set can be performed with high confidence, then the whole set has high confidence – this corresponds to the *not forbidden* modality. Second, we might stipulate that all sequences in the set have high confidence – as requested by the *free choice* modality.

Since we shall use only lower bound on (finite) sets of confidences, we require their set to be only a lower semilattice with minimal element.

Definition 2.1 Elements of the (finite) lower semilattice C are the *confidences*. The are denoted by letters p, q; moreover $p \sqcap q$ is their greatest lower bound. The minimal element of C must exists and is denoted by 0. □

As usual, $p \le q$ means $p = p \sqcap q$, thus $0 \le p$ for all $p \in C$. Actions with confidence 0 are allowed to be performed. 0 confidence means that the action is possible, but we do not think it is useful or preferable.

Now we fix the set **Act** of atomic actions, and the set **Prop** of atomic propositions. The set of *actions* is the smallest set containing all atomic actions, and closed under the following constructs: if α and β are actions, then so are $\alpha\,;\beta$, $\alpha \cup \beta$, and α^*. Actions will be denoted by small Greek letters.

Definition 2.2 The set of *propositions* is the smallest set containing all atomic propositions, and satisfy the following:

1. if X and Y are propositions, then so are $X \vee Y$ and $\neg X$;
2. if X is a proposition, α is an action and p is confidence, then $\langle\alpha\rangle^p X$ and $\langle\alpha\rangle_p X$ are propositions. □

The usual abbreviations from propositional logic will be used as well as $[\alpha]^p X$ for $\neg\langle\alpha\rangle^p\neg X$, and $[\alpha]_p X$ for $\neg\langle\alpha\rangle_p\neg X$.

The modality $\langle\alpha\rangle^p X$ expresses that X can be achieved by performing some α action with confidence $\ge p$. The dual $[\alpha]^p X$ asserts that all α actions with confidence $\ge p$ lead to a state satisfying X. This is a weak form of obligation: when executing α with confidence at least p it is obligatory to execute it in such a way that X becomes true. Since 0 is the smallest confidence, $\langle\alpha\rangle^0 X$ says that α might make X true; thus it agrees with the $\langle\alpha\rangle X$ modality of Dynamic Logic. $[\alpha]^0 X$ expresses the fact that α always makes X true (including the possibility that there is no applicable transition in α).

The other modality $\langle\alpha\rangle_p X$, originating from Meyden [3], says that X can be achieved by some α action with confidence $\le p$. Since confidences do not necessarily form an ordered set, this is not the same as saying that the confidence of such an action is not bigger than p. Now $\pi_p(\alpha) \overset{\text{def}}{=} \neg\langle\alpha\rangle_p X$ is the right notion for the free choice, expressing that if there is any α action leading to a state where X is true, then the action cannot have low confidence. Referring to the example in the introduction, if the modality "permitted" is modeled by π then "it is permitted either mail the letter of destroy it" becomes $\pi_p(\alpha \cup \beta)\mathbf{true}$, which holds if and only if both $\pi_p(\alpha)\mathbf{true}$ and $\pi_(\beta)\mathbf{true}$ are true, i.e., both actions must be permitted.

The definition of the semantics is a variation of process semantics. A *model* $\mathfrak{M}$ is a set of *worlds*, with a collection of *elementary transitions* between worlds. Each such transition has a confidence from C, expressing how desirable it is to execute it. Thus elementary transitions can be identified with triplets of the form $\langle w_0, w_1; p\rangle$ where w_0 is the source (starting point), w_1 is the destination, and $p \in C$ is its confidence.

A *transition* is a sequence $\sigma = \langle w_0, \ldots, w_k; p\rangle$ such that for all $i < k$, $\langle w_i, w_{i+1}, p_i\rangle$ is an elementary transition, and p is the greatest lower bound of $p_0, \ldots, p_{k-1}$. w_0 is the *source*, w_k is the *destination* of σ. Suppose σ_0 and σ_1 are transitions. $\sigma_0 \,;\sigma_1$ is defined only if the source of σ_1 is the same as the destination of σ_0, and then it is got by concatenating the two sequences. If α and β are sets of sequences, then

$$\alpha \,; \beta \overset{\text{def}}{=} \{\sigma_0 \,; \sigma_1 \,:\, \sigma_0 \in \alpha, \sigma_1 \in \beta\}.$$

The *empty transition*, denoted by λ, is the transition which does not contain any elementary transition at all. Its source and destination is the same world, and its confidence, $+\infty$, is bigger than any other confidence in the set C of confidences.

For each world w in $\mathfrak{M}$ there is a map τ_w assigning truth values to atomic propositions, and (possibly empty) subsets of transitions to atomic actions so that each of these transitions has w as source.

Definition 2.3 A model $\mathfrak{M}$ is a pair $\langle W, \tau\rangle$, where W is the set of worlds, and for each $w \in W$, τ_w is a map defining the value of atomic propositions and atomic actions. □

Once $\tau_w(\alpha)$ is known for atomic actions, it can be extended to every action in the usual way:

$$\begin{aligned} \tau_w(\alpha \cup \beta) &= \tau_w(\alpha) \cup \tau_w(\beta), \\ \tau_w(\alpha \,; \beta) &= \tau_w(\alpha) \,; \tau_w(\beta), \\ \tau_w(\alpha^*) &= \tau_w(\alpha)^*. \end{aligned}$$

Definition 2.4 Satisfaction for a model $\mathfrak{M} = \langle W, \tau\rangle$ and world $w \in W$ is defined as follows:

$\mathfrak{M}, w \models Q$ if $\tau_w(Q) = \textbf{true}$;

$\mathfrak{M}, w \models X \vee Y$ if $\mathfrak{M}, w \models X$ or $\mathfrak{M}, w \models Y$;

$\mathfrak{M}, w \models \neg X$ if not $\mathfrak{M}, w \models X$;

$\mathfrak{M}, w \models \langle\alpha\rangle^p X$ if for some transition in $\tau_w(\alpha)$ with destination w' and confidence $\geq p$, $\mathfrak{M}, w' \models X$;

$\mathfrak{M}, w \models \langle\alpha\rangle_p X$ if for some transition in $\tau_w(\alpha)$ with destination w' and confidence $\leq p$, $\mathfrak{M}, w' \models X$. □

A sentence X is *valid* if $\mathfrak{M}, w \models X$ for all models $\mathfrak{M}$ and worlds $w \in W$. X is *satisfiable* if for some model $\mathfrak{M}$ and world $w \in W$, $\mathfrak{M}, w \models X$; and *finitely satisfiable* if there exists a finite $\mathfrak{M}$ with this property.

3 Axiomatization

In this section we present a sound and complete axiomatization for the system introduced. The axioms and the proof of completeness follow closely that presentation in [3]. The proof of completeness yields immediately that every satisfiable sentence is finitely satisfiable, and the size of the model is at most exponential in the size of X.

The fist group of axioms list some trivial monotonic properties. In fact, they are the only ones which mix up actions of different confidence (except for those ones where stating the existence of certain action is necessary).

A1. $\langle\alpha\rangle^0\textbf{false} \equiv \textbf{false}$

A2. $\langle\alpha\rangle^q X \rightarrow \langle\alpha\rangle^p X$ for all $q \geq p$

A3. $\langle\alpha\rangle_p X \rightarrow \langle\alpha\rangle_q X$ for all $q \geq p$

A4. $\langle\alpha\rangle^p X \rightarrow \langle\alpha\rangle_p X \vee \bigvee\{\langle\alpha\rangle^q X \,:\, q > p\}$

A5. $\langle\alpha\rangle_p X \to \langle\alpha\rangle^p X \vee \bigvee\{\langle\alpha\rangle_q X \;:\; q < p\}$

In particular, it follows from A4 that if p is maximal then $\langle\alpha\rangle^p X \to \langle\alpha\rangle_p X$. Similarly, A5 gives $\langle\alpha\rangle_0 X \to \langle\alpha\rangle^0 X$. A1 and A2 together give that $\langle\alpha\rangle^p\mathbf{false}$ is always **false**. By A5 again $\langle\alpha\rangle_p\mathbf{false}$ is **false**, as otherwise the minimal p contradicting this statement would give $\langle\alpha\rangle^p\mathbf{false} \equiv \mathbf{true}$.

The dual of A5 can be looked at as induction along confidence:

$$[\alpha]^p X \wedge \bigwedge\{[\alpha]_q X \;:\; q < p\} \to [\alpha]_p X \tag{1}$$

It can be used, for example, to show

$$\vdash [\alpha]^0 X \to [\alpha]_p X. \tag{2}$$

Indeed, for $p = 0$ this is immediate from (1). For other values first use

$$[\alpha]^0 X \to [\alpha]^p X$$

which is a special case of A2, and then apply (1).

The second group defines the $\langle\alpha\rangle^p X$ modality. These axioms, expect for B5, are copies of the usual axioms for Dynamic Logic.

B1 $\langle\alpha\,;\beta\rangle^p X \equiv \langle\alpha\rangle^p\langle\beta\rangle^p X$

B2 $\langle\alpha\cup\beta\rangle^p X \equiv \langle\alpha\rangle^p X \vee \langle\beta\rangle^p X$

B3 $\langle\alpha^*\rangle^p X \equiv X \vee \langle\alpha\,;\alpha^*\rangle^p X$

B4 $\langle\alpha\rangle^p(X \vee Y) \equiv \langle\alpha\rangle^p X \vee \langle\alpha\rangle^p Y$

B5 $\langle\alpha\rangle^p X \wedge [\alpha]^0(X \to Y) \to \langle\alpha\rangle^p Y$

B6 $\langle\alpha^*\rangle^p X \to X \vee \langle\alpha^*\rangle^p(\neg X \wedge \langle\alpha\rangle^p X)$

B5 is a certain monotonic property necessary to prove Lemma 3.1. The last group of axioms deals with $\langle\alpha\rangle_p X$, which, in some sense, is a dual of $\langle\alpha\rangle^p X$.

C1 $\langle\alpha\,;\beta\rangle_p X \equiv \langle\alpha\rangle^0\langle\beta\rangle_p X \vee \langle\alpha\rangle_p\langle\beta\rangle^0 X$

C2 $\langle\alpha\cup\beta\rangle_p X \equiv \langle\alpha\rangle_p X \vee \langle\beta\rangle_p X$

C4 $\langle\alpha\rangle_p(X \vee Y) \equiv \langle\alpha\rangle_p X \vee \langle\alpha\rangle_p Y$

C5 $\langle\alpha\rangle_p X \wedge [\alpha]^0(X \to Y) \to \langle\alpha\rangle_p Y$

C6 $\langle\alpha^*\rangle_p X \equiv \langle\alpha^*\rangle^0\langle\alpha\rangle_p\langle\alpha^*\rangle^0 X$

(Observe that there is no axiom labeled C3.) B1 says that $\alpha\,;\beta$ has confidence at least p just in case if both α and β have confidence $\geq p$. By C1, $\alpha\,;\beta$ has confidence at most p, if either α or β has confidence $\leq p$. B6 is the usual induction axiom, which can be more familiar in he dual form

$$X \wedge [\alpha^*]^p(X \to [\alpha]^p X) \to [\alpha^*]^p X,$$

i.e., if X is true in the initial world and in each α^* accessible world it inherits to all α-next world, then X is true in all α^* reachable worlds. Axiom C6 expresses the fact that if a sequence of transitions has low confidence then at least one element must have low confidence. In dual form

$$[\alpha^*]^0[\alpha]_p[\alpha^*]^0 X \equiv [\alpha^*]_p X.$$

Besides these, all instances of propositional tautologies are axioms. As inference, we have *modus ponens* and *generalization*:

$$X, X \to Y \vdash Y \quad \text{and} \quad X \vdash [\alpha]^0 X.$$

X is (syntactically) *consistent* if not $\vdash \neg X$. Note that if $X_1 \vee X_2 \vee \ldots \vee X_n$ is consistent then one of the disjuncts is also consistent. Finally, if $\vdash X \to Y$ then we write $X \leq Y$.

Lemma 3.1 *If $\vdash X \equiv Y$ then $\vdash W(X) \equiv W(Y)$, where $W(Y)$ is the result of substituting one or more occurrences of X by Y in $W(X)$.*

Proof By B5, C5, and generalization, $\vdash X \equiv Y$ implies $\vdash \langle\alpha\rangle^p X \equiv \langle\alpha\rangle^p Y$ and $\vdash \langle\alpha\rangle_p X \equiv \langle\alpha\rangle_p Y$. From here the lemma follows by simple induction. □

4 Completeness

The proof here is a slight modification of the one found in [3] tailored to our purposes. We wish to show that if Z is consistent, then there is a (finite) model $\mathfrak{M}$ and a world w in $\mathfrak{M}$ such that $\mathfrak{M}, w \models Z$. To this end we define the *deontic Fisher-Ladner closure* $cl(Z)$ of Z [5] as follows.

Definition 4.1 $cl(Z)$ is the smallest set of deontic formulas containing Z which satisfies the following conditions:

1. if $X \vee Y \in cl(Z)$ then $X \in cl(Z)$ and $Y \in cl(Z)$;
2. if $\neg X \in cl(Z)$ then $X \in cl(Z)$; if X does not start with $\neg$ and $X \in cl(Z)$ then $\neg X \in cl(Z)$;
3. if $\langle\alpha\rangle^p X \in cl(Z)$ or $\langle\alpha\rangle_p X \in cl(Z)$ then $X \in cl(Z)$;
4. if the left hand side of B1–B4, C1–C4 is in $cl(Z)$, then the corresponding right hand side is also in $cl(Z)$;
5. if $\langle\alpha^*\rangle^p X \in cl(Z)$ then $\langle\alpha\rangle^p X \in cl(Z)$;
6. if $\langle\alpha^*\rangle_p X \in cl(Z)$ then $\langle\alpha^*\rangle^0\langle\alpha\rangle_p\langle\alpha^*\rangle^0 X \in cl(Z)$. □

Of course, $cl(Z)$ is always finite, however its size can be exponential in the size of Z. (The size can increase to exponential because of rules 4 and 5. If $\langle\alpha^*\rangle^p X \in cl(Z)$ then both $\langle\alpha\rangle^p X$ and $\langle\alpha\rangle^p\langle\alpha^*\rangle^p X$ are in $cl(Z)$. Consequently if Z is of the form $\langle\alpha^{**\cdots*}\rangle^p X$ with n stars, then $cl(Z)$ has at least 2^n elements. If we stipulate $\alpha^{**} = \alpha^*$ then the size of $cl(Z)$ can still be quadratic.)

An *atom* is a maximal consistent subset of $cl(Z)$.

There is at least one atom $\leq Z$ since Z is equivalent to the disjunction of all atoms below Z. Atoms will be denoted by A, B, C, and D. By maximality, for every atom A and $X \in cl(Z)$, either $A \leq X$ or $A \leq \neg X$.

The worlds of our model $\mathfrak{M}$ are labeled by pairs (A, p) where A is an atom, and $p \in C$ is a confidence. All elementary transitions arriving at (A, p) have confidence p; all outgoing transitions from (A, p) depend only on A and not on p, i.e. exactly the same deontic formulas are true in (A, p) than in (A, q). For an atomic proposition Q let

$$\tau(A,p)(Q) = \textbf{true} \quad if \quad A \leq Q.$$

If a is an atomic action, then its interpretation $\tau_{(A,p)}(a)$ consists of those elementary transitions with source (A, p) and destination (B, q) for which

$$A \wedge \langle a\rangle^q B \wedge \langle a\rangle_q B$$

is consistent. This concludes the definition of $\mathfrak{M}$.

Now the main result of this section is the following

Theorem 4.2 *For any $X \in cl(Z)$ and state A, $(A, p) \models X$ iff $A \leq X$.*

From here the completeness of our axiom system follows immediately, since at least one atom is below Z.

The proof of the theorem proceeds by a series of definitions and lemmas. Since it is very similar to the completeness proof given in [5], we give only those parts which differ essentially.

First, to ease the description, we write $A\langle\alpha\rangle^p B$ to indicate that for some q and r there is an α transition from world (A, q) to (B, r) with confidence at least p. Similarly, $A\langle\alpha\rangle_p B$ means that such an α transition exists with confidence $\leq p$. In particular, $A\langle\lambda\rangle^p A$ always holds, as the confidence of the empty transition λ exceeds all other confidences.

Lemma 4.3 *if $A \wedge \langle\alpha\rangle^p B$ is consistent, then $A\langle\alpha\rangle^p B$.*

Proof By induction on the complexity of α. The base case reduces to showing that if $A \wedge \langle a\rangle^p B$ is consistent, then for some $q \geq p$,

$$A \wedge \langle a\rangle^q B \wedge \langle a\rangle_q B$$

is also consistent. Suppose not. Then $A \wedge \langle a\rangle^q B \vdash \neg\langle a\rangle_q B$ for all $q \geq p$. But this is impossible, as by A4, if q is maximal then $\langle a\rangle^q B \rightarrow \langle a\rangle_q B$.

For the remaining cases we follow the treatment of [5]. Suppose the statement is true for α and β, and $A \wedge \langle\alpha\,;\beta\rangle^p B$ is consistent. Then, by B1 and B4, this formula is equivalent to

$$\bigvee\nolimits_C \left\{A \wedge \langle\alpha\rangle^p(C \wedge \langle\beta\rangle^p B)\right\}$$

where C runs over all atoms. Thus for at least one atom C both $A \wedge \langle\alpha\rangle^p C$ and $C \wedge \langle\beta\rangle^p B$ are consistent which gives the lemma for $\alpha\,;\beta$.

Similarly, B2 shows that $A \wedge \langle\alpha \cup \beta\rangle^p B$ is consistent iff either $A \wedge \langle\alpha\rangle^p B$ or $A \wedge \langle\beta\rangle^p B$ is so. This gives the result for $\alpha \cup \beta$.

Finally we consider the case α^*, i.e., assume $A \wedge \langle\alpha^*\rangle^p B$ is consistent. Split the atoms into two sets S and T such S is the smallest possible, $A \in S$, and whenever $C \in S$ and $C \wedge \langle\alpha\rangle^p D$ is consistent then $D \in S$ as well. Clearly, for arbitrary $C \in S$, $A\langle\alpha^*\rangle^p C$, thus it is enough to show that for $D \in T$, $A \wedge \langle\alpha^*\rangle^p D$ is inconsistent. First note that $C \wedge \langle\alpha\rangle^p D$ is inconsistent whenever $C \in S$ and $D \in T$, consequently

$$\bigvee \left\{C \wedge \langle\alpha\rangle^p D \,:\, C \in S \text{ and } D \in T\right\} \equiv (\bigvee S) \wedge \langle\alpha\rangle^p(\bigvee T)$$

is inconsistent as well. As the disjoint sets S and T contain all atoms, if Y denotes $\bigvee S$, then $\bigvee T$ is the same as $\neg Y$, thus the above inconsistency gives $\vdash Y \rightarrow [\alpha]^p Y$. By generalization, $\vdash [\alpha^*]^0(Y \rightarrow [\alpha]^p Y)$, and by A2 $\vdash [\alpha^*]^p(Y \rightarrow [\alpha]^p Y)$. Using that $A \in S$, i.e., $\vdash A \rightarrow Y$ and the dual of B6, we get $\vdash A \rightarrow [\alpha^*]^p Y$, i.e. $\vdash A \rightarrow \neg\langle\alpha^*\rangle^p(\bigvee T)$. It means that no $A \wedge \langle\alpha^*\rangle^p D$ can be consistent when $D \in T$, as was claimed. □

Lemma 4.4 *If $A \wedge \langle\alpha\rangle_p B$ is consistent, then $A\langle\alpha\rangle_p B$.*

Proof Almost word by word the previous proof. In the base case if

$$A \wedge \langle a\rangle^q B \wedge \langle a\rangle_q B$$

were not consistent for every $q \leq p$, then $A \wedge \langle a\rangle_q B \vdash \neg\langle a\rangle^q B$. But this is impossible, as by A5, $\vdash \langle\alpha\rangle_0 B \rightarrow \langle\alpha\rangle^0 B$ and $0 \leq p$.

Now assume the statement is true for α and β, and $A \wedge \langle\alpha\,;\beta\rangle_p B$ is consistent. By C1, C4 and B4 this formula is equivalent to

$$\bigvee\nolimits_C \left\{A \wedge \langle\alpha\rangle^0(C \wedge \langle\beta\rangle_p B)\right\} \vee \bigvee\nolimits_D \left\{A \wedge \langle\alpha\rangle_p(D \wedge \langle\beta\rangle^0 B\right\}$$

where C and D runs over all atoms. Thus either both $A \wedge \langle\alpha\rangle^0 C$ and $C \wedge \langle\beta\rangle_p B$ are consistent, or both $A \wedge \langle\alpha\rangle_p D$ and $D \wedge \langle\beta\rangle^0 B$ are consistent. In both cases by induction and by the previous lemma we are done.

The case for $\alpha \cup \beta$ requires no new ideas.

Finally assume $A \wedge \langle\alpha^*\rangle_p B$ is consistent. Then, by C6, so is $A \wedge \langle\alpha^*\rangle^0\langle\alpha\rangle_p\langle\alpha^*\rangle^0 B$, which (using B4 and C4) is equivalent to

$$\bigvee\nolimits_{C,D} A \wedge \langle\alpha^*\rangle^0\big(C \wedge \langle\alpha\rangle_p(D \wedge \langle\alpha^*\rangle^0 B)\big)$$

where C and D runs over all atoms. Thus for some atoms C and D all of $A \wedge \langle\alpha^*\rangle^0 C$, $C \wedge \langle\alpha\rangle_p D$ and $D \wedge \langle\alpha^*\rangle^0 B$ are consistent. Using the induction hypothesis and the previous lemma we are done. □

Lemma 4.5 *For any $\langle\alpha\rangle^p X \in cl(Z)$ and atom A, $A \leq \langle\alpha\rangle^p X$ if and only if $A\langle\alpha\rangle^p B$ for some $B \leq X$.*

Proof If $A \leq \langle\alpha\rangle^p X$ then $A \wedge \langle\alpha\rangle^p B$ is consistent for some atom extending X, and the result follows from Lemma 4.3.

On the other direction suppose $A\langle\alpha\rangle^p B$ and $B \leq X$. If α is atomic, say $\alpha = a$, then, by the definition of $A\langle a\rangle^p B$, $A \wedge \langle a\rangle^q B \wedge \langle a\rangle_q B$ is consistent for some $p \leq q$. Consequently, by A2, $A \wedge \langle a\rangle^p B$ is also consistent, therefore so is $A \wedge \langle a\rangle^p X$, which gives $A \leq \langle a\rangle^p X$.

If $A\langle\alpha \cup \beta\rangle^p B$ then either $A\langle\alpha\rangle^p B$ or $A\langle\beta\rangle^p B$, and both $\langle\alpha\rangle^p X \in cl(Z)$ and $\langle\beta\rangle^p X \in cl(Z)$. Thus we can apply induction to get

$$A \leq \langle\alpha\rangle^p X \leq \langle\alpha \cup \beta\rangle^p X \quad \text{or} \quad A \leq \langle\beta\rangle^p X \leq \langle\alpha \cup \beta\rangle^p X.$$

If $A\langle\alpha;\beta\rangle^p B$ then for some atom C we have $A\langle\alpha\rangle^p C$ and $C\langle\beta\rangle^p B$. As $\langle\beta\rangle^p X \in cl(Z)$, induction gives $C \leq \langle\beta\rangle^p X$. Now, setting $Y = \langle\beta\rangle^p X$, $\langle\alpha\rangle^p Y \in cl(Z)$ and $C \leq Y$, thus the induction gives

$$A \leq \langle\alpha\rangle^p Y \equiv \langle\alpha\rangle^p\langle\beta\rangle^p X \equiv \langle\alpha\,;\beta\rangle^p X,$$

as required.

Finally, suppose there are atoms so that $A = A_1$, $A_i\langle\alpha\rangle^p A_{i+1}$ and $A_n = B$, $B \leq X$ and $\langle\alpha^*\rangle^p X \in cl(Z)$. As, by B3, $X \leq \langle\alpha^*\rangle^p X$, $A_n \leq X \leq \langle\alpha^*\rangle^p$. By assumption, $\langle\alpha\rangle^p\langle\alpha^*\rangle^p X \in cl(Z)$ as well, thus by induction

$$A_{n-1} \leq \langle\alpha\rangle^p\langle\alpha^*\rangle^p X \leq \langle\alpha^*\rangle^p X$$

by B1 and B3. Continuing backward we get $A \leq \langle\alpha^*\rangle^p X$, as was required. □

Lemma 4.6 *For any $\langle\alpha\rangle_p X \in cl(Z)$ and atom A, $A \leq \langle\alpha\rangle_p X$ if and only if $A\langle\alpha\rangle_p B$ for some $B \leq X$.*

Proof The proof follows that of the previous lemma with the only differences at handling $\langle\alpha\,;\beta\rangle_p$ and $\langle\alpha^*\rangle_p$. First assume $A\langle\alpha;\beta\rangle_p B$. Then there is an atom C such that either $A\langle\alpha\rangle^0 C$ and $C\langle\beta\rangle_p B$, or $A\langle\alpha\rangle_p C$ and $C\langle\beta\rangle^0 B$. In the first case $\langle\beta\rangle_p X \in cl(Z)$, thus $C \leq \langle\beta\rangle_p X$ by induction. Also, $\langle\alpha\rangle^0\langle\beta\rangle_p X \in cl(Z)$, therefore $A \leq \langle\alpha\rangle^0\langle\beta\rangle_p X \leq \langle\alpha\,;\beta\rangle_p X$ by C1. In the other case we use that $\langle\beta\rangle^0 X$ and $\langle\alpha\rangle_p\langle\beta\rangle^0 X$ are also in $cl(Z)$.

As the last case, suppose there are atoms C and D such that $A\langle\alpha^*\rangle^0 C$, $C\langle\alpha\rangle_p D$, $D\langle\alpha^*\rangle^0 B$, and $B \leq X$. Then by Lemma 4.4 $D \leq \langle\alpha^*\rangle^0 X$; by induction $C \leq \langle\alpha\rangle_p\langle\alpha^*\rangle^0 X$, and applying Lemma 4.4 again we get $A \leq \langle\alpha^*\rangle^0\langle\alpha\rangle_p\langle\alpha^*\rangle^0 X$. By C6 we are done. □

5 Conclusion

It was not our goal to discuss the philosophical significance (if any) of our proposal. We wanted only to generalize the Dynamic Logic of Permission introduced in Meyden [3], and give a more natural axiomatization. In the axioms the duality between "free choice" and "not forbidden" is more transparent. Also, producing practical applications and convincing examples of the usefulness of our multi-level permissions is left to the interested reader.

It is interesting to note that a general separation property follows almost immediately from the method of our proof of completeness. To state this property, suppose that C_1 and C_2 are downward closed subsets of the confidence lattice C so that $C = C_1 \cup C_2$ (set theoretical union). Then C_1, C_2 as well as $C_1 \cap C_2$ are also a semilattice. Denote by $f(c)$ the set of deontic formulas using confidence values form C; obviously $F(C_1 \cap C_2) = f(C_1) \cap F(C_2)$.

Theorem 5.1 *Let $X_1 \in F(C_1)$, and $X_2 \in F(C_2)$. Then the following are equivalent:*

1. *there is no formula $Y \in F(C_1) \cap F(C_2)$ so that $X_1 \vdash Y$ and $X_2 \vdash \neg Y$;*

2. *There are models $\mathfrak{M}_1$ and $\mathfrak{M}_2$ differing only in the confidence of the elementary transitions so that $\mathfrak{M}_1 \models X_1$ and $\mathfrak{M}_2 \models X_2$.*

Proof The implication 2 ⇒ 1 is obvious, so we concentrate on the other direction. First, if 1 is true, then $X_1 \wedge X_2$ is consistent. This follows, e.g., from the interpolation theorem for the first order calculus [1], but can be checked directly, too. Now let $\mathfrak{M}$ be the model constructed for $X_1 \wedge X_2$ in section 4. We claim that the confidence of elementary transitions between the worlds can be reassigned so that $\mathfrak{M}$ becomes a C_1 model for X_1. By symmetry, then the same can be done for X_2, thus the theorem follows.

Let a be an atomic action. By definition of $\mathfrak{M}$, if we have an a-transition from world (A, p) to (B, q) then it has confidence q. If q is in C_1 then do nothing. If q is not in C_1 then we have to reassign the confidence of this transition. We claim that in this case there is an a-transition from (A, p) to (B', q') for some $q' \in C_1$ and world B' where B' and B agrees on all C_1-atoms. In this case we can safely change the confidence of the $(A, p) \xrightarrow{a} (B, q)$ transition to q' since worlds (B, q) and (B', q') are C_1-isomorphic, and the presence of more than one transition in $\tau_{(A,p)}(a)$ cannot be checked by any deontic formula.

Thus we have to verify our last claim only. If there is an a-transition from (A, p) to (B, q') for some $q' \in C_1 \cap C_2$ then we are done. If not, then let $r \in C_1 \cap C_2$ be the largest element below q. Then in (A, p) the following formula holds:

$$\langle a \rangle^r B' \wedge \neg \langle a \rangle_r B' \tag{3}$$

where B' is the C_1 part of B. If no a-transition exists from (A, p) to (B', q') for some $q' \in C_1$ then (3) would separate X_1 and X_2, contradicting our assumption. □

References

[1] J. Barwise (ed.), *Handbook of Mathematical Logic*, North Holland (1977)

[2] L. McCarty, Permissions and obligations, in *Proceedings of IJCAI'83* (1983) pp 287–294

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

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

[5] D. Kozen and R. Parikh, An elementary proof of the completeness of PDL *Theoretical Computer Science* **14** (1981), 113–118