STUDIA UNIV. BABEŞ–BOLYAI, INFORMATICA, Volume **LIV**, Number 1, 2009

PROVING THE DECIDABILITY OF THE PDL×PDL PRODUCT LOGIC

LÁSZLÓ ASZALÓS AND PHILIPPE BALBIANI

Abstract. The propositional dynamic logic (PDL) is an adequate tool to write down programs. In a previous article we used PDL to formulate cryptographic protocols as parallel programs. In these protocols at least two agents/individuals exchange messages, so we needed to use product logic to formulate the parallel actions. Ágnes Kurucz proved that S5×S5×S5 — which is the simplest triple product logic — is undecidable, hence it follows that PDL×PDL×PDL is undecidable, too. It is easy to show that the PDL logic (without the star operator) is decidable, so it is an interesting problem, that the PDL×PDL product logic is decidable or not.

1. Introduction

Authentication protocols emerged from numerous works of computer scientists and their use has become common in the science and study of methods of exchanging keys. They are basically sequences of message exchanges, whose purpose is to assure users that communications do not leak confidential data. Indeed, there is a wide variety of protocols that have been specified and implemented, from protocols with trusted third party, to protocols with public key and, even more generally, hybrid protocols. The one drawback is that many of them have been shown to be flawed, from which one may explain the great deal of attention devoted to the formal verification of security properties of protocols. Examples of protocols can be found in [4].

Received by the editors: December 6, 2008.

2000 *Mathematics Subject Classification.* 03B45, 94A60.

1998 *CR Categories and Descriptors.* F.4.1 [**Mathematical logic**]: model logic – *product of propositional dynamic logics*; D.4.6 [**Security and protection**]: Authentication – *formal verification of authentication protocols* .

Key words and phrases. Mathematical logic, Decidability, PDL×PDL product logic, Formal verification.

This paper has been presented at the 7th Joint Conference on Mathematics and Computer Science (7th MaCS), Cluj-Napoca, Romania, July 3-6, 2008.

In the literature, the most popular logic-based formal approach to the analysis of authentication protocols is perhaps the modal BAN calculus introduced by Burrows, Abadi and Needham [3]. From the point of view of computer science, a virtue of BAN is that it allows static characterization of epistemic concepts. In spite of its success in finding flaws or redundancies in some well-known protocols, the effectiveness of BAN as a formal method for the analysis of authentication protocols has been a source of debate, see [9] for details. The problem with the BAN logic is that it explicitly excludes time. On the other hand there is no way to represent actions performed by users. Communication, by its nature, refers to time, and its properties are naturally expressed in terms of actions like sending and receiving messages. When devising a protocol, we usually think of some property that we want the protocol to satisfy. We are mainly interested in the correctness of a protocol with respect to epistemic properties between two users like the arranging of a secret key known only to them. Therefore, our emphasis is on the interplay between knowledge and action. This leads us to consider a language that allows to express notions of knowledge and actions in a straightforward way: the language of modal logic.

We can treat protocols as programs, so we used the propositional dynamic logic (PDL) [7] as a starting point. It allows for us to examine properties of the protocol using logic. Protocols are not just sole programs, but a set of programs. Usually two or three programs run parallel when a protocol executed: the program of Alice, of Bob and maybe program of Charlie, if we use the the traditional names of the cryptography. To handle the parallel execution of programs, we developed the product logic PDL×PDL, using the construction of Gabbay and Shehtman [5, 6].

We would use the logic PDL×PDL to examine real protocols, so the decidability of the logic is very important. From [8] we know that S5×S5×S5 — which is the simplest triple product logic — is undecidable, so the examination of PDL×PDL×PDL unnecessary. The original PDL logic is decidable. What is the status of our construction which is between in PDL and PDL×PDL×PDL? We will prove in this article that PDL×PDL is decidable.

In the following section we introduce the logic, PDL×PDL, and after we show the method of quasimodels developed by Wolter and Zakharyaschev and explained in [5].

2. PDL×PDL logic

The PDL logic is a logic of actions, so at first we define the set of actions. We have a finite set of atomic actions, its elements are denoted with π_i. Two atomic actions are special: the sending and receiving messages. They are denoted with `send` and `rec`. For our proofs the structure of messages are indifferent. In our previous papers [1, 2] we discussed the structure of messages in detail. To construct complicated actions we can use the operators of test, sequence and selections, denoted by ?, semicolon and ∪, respectively.

$$\alpha \;\leftrightharpoons\; \lambda \mid \pi_k \mid A? \mid \alpha;\beta \mid \alpha\cup\beta \mid \mathtt{send}(m) \mid \mathtt{rec}(m)$$

We can define the formulae based on the set of atomic formulae, by using the usual logical connectives and the modalities constructed from a pair of actions:

$$A \;\leftrightharpoons\; p_k \mid \neg A \mid A \vee B \mid \langle \alpha_1 \parallel \alpha_2 \rangle A$$

For the semantics, we use a variant of the Kripke model. We have two agents, so the global state is build up from local states. The model $\mathcal{M}$ is a (W_1, W_2, r, R, V) tuple where W_1 and W_2 are the set of local states (possible worlds), r and R is a family of relations on W_i (r_i, $R_i \subseteq W_i \times W_i$), and V is a valuation on $W_1 \times W_2$ ($V(p_j) \subseteq W_1 \times W_2$). Given a model $\mathcal{M}$ we define the relation $R_{\alpha\|\beta}$ and the $(s,t,c) \models_{\mathcal{M}} A$ truth-relation by a parallel induction for any states $s, s' \in W_1$, $t, t' \in W_2$, actions α, β and formula A as follows:

- $(s,t,c)\ R_{\lambda\|\lambda}\ (s',t',c')$ iff $s = s',\ t = t',\ c = c'$;
- $(s,t,c)\ R_{\pi_i\|\lambda}\ (s',t',c')$ iff $sr_is',\ t = t',\ c = c'$;
- $(s,t,c)\ R_{\lambda\|\pi_i}\ (s',t',c')$ iff $s = s',\ tR_it',\ c = c'$;
- $(s,t,c)\ R_{A?\|\lambda}\ (s',t',c')$ iff $s = s',\ t = t',\ c = c',\ (s,t,c) \models_{\mathcal{M}} A$;
- $(s,t,c)\ R_{\lambda\|A?}\ (s',t',c')$ iff $s = s',\ t = t',\ c = c',\ (s,t,c) \models_{\mathcal{M}} A$;
- $(s,t,c)\ R_{\mathtt{send}(m)\|\lambda}\ (s',t',c')$ iff $s = s',\ t = t'$, and if $c = (c_1, c_2)$, then $c' = (c_1, c_2 \star m)$;
- $(s,t,c)\ R_{\lambda\|\mathtt{send}(m)}\ (s',t',c')$ iff $s = s',\ t = t'$, and if $c = (c_1, c_2)$, then $c' = (c_1 \star m, c_2)$;
- $(s,t,c)\ R_{\mathtt{rec}(m)\|\lambda}\ (s',t',c')$ iff $s = s',\ t = t'$, and if $c' = (c_1, c_2)$, then $c = (m \star c_1, c_2)$;
- $(s,t,c)\ R_{\lambda\|\mathtt{rec}(m)}\ (s',t',c')$ iff $s = s',\ t = t'$, and if $c' = (c_1, c_2)$, then $c = (c_1, m \star c_2)$;
- $R_{\varphi;\alpha\|\psi;\beta} \;\leftrightharpoons\; (R_{\varphi\|\lambda} \circ R_{\alpha\|\psi;\beta}) \cup (R_{\lambda\|\psi} \circ R_{\varphi;\alpha\|\beta})$ where φ_i and ψ_j are atomic action, test, send or receive actions;
- $R_{\alpha(\alpha_1\cup\alpha_2)\|\beta} \;\leftrightharpoons\; R_{\alpha(\alpha_1)\|\beta} \cup R_{\alpha(\alpha_2)\|\beta}$;
- $R_{\alpha\|\beta(\beta_1\cup\beta_2)} \;\leftrightharpoons\; R_{\alpha\|\beta(\beta_1)} \cup R_{\alpha\|\beta(\beta_2)}$.
- $(s,t,c) \models_{\mathcal{M}} p_i$ iff $(s,t) \in V(p_i)$
- $(s,t,c) \models_{\mathcal{M}} \neg A$ iff $(s,t,c) \not\models_{\mathcal{M}} A$.
- $(s,t,c) \models_{\mathcal{M}} A \vee B$ iff $(s,t,c) \models_{\mathcal{M}} A$ or $(s,t,c) \models_{\mathcal{M}} B$.

- $(s,t,c) \models_{\mathcal{M}} \langle \alpha \parallel \beta \rangle A$, if there exists a triple (s',t',c') such that (s,t,c) $R_{\alpha_1 \parallel \alpha_2}$ (s',t',c') and $(s',t',c') \models_{\mathcal{M}} A$

We say that formula A is *satisfiable* in model $\mathcal{M}$ if there is exists $s \in W_1$ and $t \in W_2$ such that $(s,t,(\varepsilon,\varepsilon)) \models_{\mathcal{M}} A$; and we say that formula A is *valid* in model $\mathcal{M}$ if for all $s \in W_1$ and $t \in W_2$, $(s,t,(\varepsilon,\varepsilon)) \models_{\mathcal{M}} A$.

3. Quasimodel

To prove the decidability of the PDL×PDL logic, we follow the method described in [5]. At first we need the concept of the subformula. The standard definition is not suitable for us, so we use a variant. The *Fischer-Ladner closure of* φ $(flc(\varphi))$ defined as

- if $\psi \vee \chi \in flc(\varphi)$ then $\psi \in flc(\varphi)$, $\chi \in flc(\varphi)$;
- if $\neg\psi \in flc(\varphi)$ then $\psi \in flc(\varphi)$;
- if $\langle \alpha \parallel \beta \rangle \psi \in flc(\varphi)$ then $\psi \in flc(\varphi)$;
- if $\langle \alpha(\alpha_1 \cup \alpha_2) \parallel \beta \rangle \psi \in flc(\varphi)$ then $\langle \alpha(\alpha_1) \parallel \beta \rangle \psi \in flc(\varphi)$, $\langle \alpha(\alpha_2) \parallel \beta \rangle \psi \in flc(\varphi)$;
- if $\langle \alpha \parallel \beta(\beta_1 \cup \beta_2) \rangle \psi \in flc(\varphi)$ then $\langle \alpha \parallel \beta(\beta_1) \rangle \psi \in flc(\varphi)$, $\langle \alpha \parallel \beta(\beta_2) \rangle \psi \in flc(\varphi)$;
- if $\langle \pi; \alpha \parallel \beta \rangle \psi \in flc(\varphi)$ then $\langle \pi \parallel \lambda \rangle \langle \alpha \parallel \beta \rangle \psi \in flc(\varphi)$, where π is an atomic action or a test;
- if $\langle \alpha \parallel \pi; \beta \rangle \psi \in flc(\varphi)$ then $\langle \lambda \parallel \pi \rangle \langle \alpha \parallel \beta \rangle \psi \in flc(\varphi)$, where π is an atomic action or a test;
- if $\langle \psi? \parallel \lambda \rangle \chi \in flc(\varphi)$ or $\langle \lambda \parallel \psi? \rangle \chi \in flc(\varphi)$ then $\psi \in flc(\varphi)$, and $\chi \in flc(\varphi)$.

Type t for φ is a Boolean saturated subset t of $flc(\varphi)$, satisfying the following conditions:

(t_1) $\langle \lambda \parallel \lambda \rangle \psi \in t$ iff $\psi \in t$ for all $\langle \lambda \parallel \lambda \rangle \psi \in flc(\varphi)$;
(t_2) $\langle \pi; \alpha \parallel \lambda \rangle \psi \in t$ iff $\langle \pi \parallel \lambda \rangle \langle \alpha \parallel \lambda \rangle \psi \in t$ for all $\langle \pi; \alpha \parallel \lambda \rangle \psi \in flc(\varphi)$;
(t_3) $\langle \lambda \parallel \pi; \beta \rangle \psi \in t$ iff $\langle \lambda \parallel \pi \rangle \langle \lambda \parallel \beta \rangle \psi \in t$ for all $\langle \lambda \parallel \pi; \beta \rangle \psi \in flc(\varphi)$;
(t_4) $\langle \pi; \alpha \parallel \pi'; \beta \rangle \psi \in t$ iff either$\langle \pi \parallel \lambda \rangle \langle \alpha \parallel \pi'; \beta \rangle \psi \in t$ or $\langle \lambda \parallel \pi' \rangle \langle \pi; \alpha \parallel \beta \rangle \psi \in t$ for all $\langle \pi; \alpha \parallel \pi'; \beta \rangle \psi \in flc(\varphi)$;
(t_5) $\langle \alpha(\alpha_1 \cup \alpha_2) \parallel \beta \rangle \psi \in t$ iff either$\langle \alpha(\alpha_1) \parallel \beta \rangle \psi \in t$ or $\langle \alpha(\alpha_2) \parallel \beta \rangle \psi \in t$ for all $\langle \alpha(\alpha_1 \cup \alpha_2) \parallel \beta \rangle \psi \in flc(\varphi)$;
(t_6) $\langle \alpha \parallel \beta(\beta_1 \cup \beta_2) \rangle \psi \in t$ iff either$\langle \alpha \parallel \beta(\beta_1) \rangle \psi \in t$ or $\langle \alpha \parallel \beta(\beta_2) \rangle \psi \in t$ for all $\langle \alpha \parallel \beta(\beta_1 \cup \beta_2) \rangle \psi \in flc(\varphi)$;
(t_7) $\langle \psi? \parallel \lambda \rangle \chi \in t$ iff $\psi \in t$ and $\chi \in t$ for all $\langle \psi? \parallel \lambda \rangle \chi \in flc(\varphi)$;
(t_8) $\langle \lambda \parallel \psi? \rangle \chi \in t$ iff $\psi \in t$ and $\chi \in t$ for all $\langle \lambda \parallel \psi? \rangle \chi \in flc(\varphi)$.

Modal depth of a formula φ ($md(\varphi)$) is defined as usual:

- $md(p_i) = md(\top) = 0$;
- $md(\neg\varphi) = md(\varphi)$;
- $md(\varphi \vee \psi) = \max(md(\varphi), md(\psi))$;
- $md([\alpha \,\|\, \beta]\varphi) = md(\langle\alpha \,\|\, \beta\rangle\varphi)$;
- $md(\langle\lambda \,\|\, \lambda\rangle\varphi) = md(\varphi)$;
- $md(\langle\alpha(\alpha_1 \cup \alpha_2) \,\|\, \beta\rangle\varphi) = \max(md(\langle\alpha(\alpha_1) \,\|\, \beta\rangle\varphi), md(\langle\alpha(\alpha_2) \,\|\, \beta\rangle\varphi))$;
- $md(\langle\alpha \,\|\, \beta(\beta_1 \cup \beta_2)\rangle\varphi) = \max(md(\langle\alpha \,\|\, \beta(\beta_1)\rangle\varphi), md(\langle\alpha \,\|\, \beta(\beta_2)\rangle\varphi))$;
- $md(\langle\pi;\alpha \,\|\, \beta\rangle\varphi) = md(\langle\alpha \,\|\, \pi;\beta\rangle\varphi) = 1 + md(\langle\alpha \,\|\, \beta\rangle\varphi)$.

An n-frame $\mathcal{F} = (W, R_1, \ldots, R_n)$ is called *rooted*, if there is a $w_0 \in W$ such that $W = \{w \in W | w_0 R^* w\}$, where $R = \bigcup_{1 \le j \le n} R_j$. Such a w_0 is called a *root of* $\mathcal{F}$. A rooted frame $\mathcal{F} = (W, R_1, \ldots, R_n)$ is said to be a *tree* if all the R_j are pairwise disjoint and for every $x \in W$, the set $W_x = \{y \in W | yR^*x\}$ is finite and linearly ordered by the reflexive and transitive closure R^* of the relation R (its restriction to W_x, to be more precise). $\mathcal{F}$ is called *intransitive* if for any R_j, R_k $(1 \le j, k \le n)$ we have $\forall x, y, z \in W(xR_jy \wedge yR_kz \to \neg xR_kz \wedge \neg xR_jz)$. A path of length l from x to y in $\mathcal{F}$ is a sequence $(x_0, \ldots, x_l)$ such that $x_0 = x$, $x_l = y$ and $x_kR_jx_{k+1}$ for each $k < l$ and some j, $1 \le j \le n$. The length of the path from the root of $\mathcal{F}$ to x is called the *co-depth* of x. The *depth* of $\mathcal{F}$ is the maximum of co-depth of x $(x \in W)$, if this maximum exists. By the *depth* of x in $\mathcal{F}$ we understand the depth of the subtree of $\mathcal{F}$ with root x. The *Quasistate candidate for* φ is a pair $((T, R_1, \ldots, R_k), t)$, where $(T, R_1, \ldots, R_k)$ is a finite intransitive tree of depth $md(\varphi)$, and t is a labeling function associating with each $x \in T$ a type $t(x)$ for φ. $((T, R_1, \ldots, R_k), t)$ is a *quasistate for* φ if

(qm1) for all $x \in T$ and $\langle\lambda \,\|\, \pi_i\rangle\psi \in flc(\varphi)$: $\langle\lambda \,\|\, \pi_i\rangle\psi \in t(x)$ iff there exists a $y \in T$ such that xR_iy and $\psi \in t(y)$.

(qm1') for all x_0, x_1, $x_2 \in T$ such that $x_0R_ix_1$, $x_0R_ix_1$, and $x_1 \neq x_2$ the structures $((T^{x_1}, R_1^{x_1}, \ldots, R_k^{x_1}), t^{x_1})$ and $((T^{x_2}, R_1^{x_2}, \ldots, R_k^{x_2}), t^{x_2})$ are not isomorphic. (Two quasistate candidates $((T, <_1, \ldots, <_n), t)$ and $((T', <_1', \ldots, <_n'), t')$ are called *isomorphic* if there is an isomorphism f between the trees $(T, <_1, \ldots, <_n)$ and $(T', <_1', \ldots, <_n')$ such that $t(x) = t'(f(x))$, for all $x \in T$.)

A *basic structure for* φ *of depth* m is a pair $(\mathcal{F}, q)$, such that $\mathcal{F} = (W, r_1, \ldots, r_k)$ and q is a function associating with each world $w \in W$ and each message $c = (c_1, c_2)$ a quasistate $q(w, c) = ((T_w^c, R_{w,1}^c, \ldots, R_{w,k}^c), t_w^c)$ for φ such that the depth of each $(T_w^c, R_{w,i}^c)$ is m. Let $(\mathcal{F}, q)$ be a basic structure for φ of depth m and let $l \le m$. An *l-run through* $(\mathcal{F}, q)$ is a function ρ giving for each $w \in W$ and the list of messages c a point $\rho(w, c) \in T_w^c$ of co-depth l. Given a set $\mathcal{R}$ of runs we denote by $\mathcal{R}_l$ the set of all l-runs from $\mathcal{R}$. A run ρ is called *coherent*, if for all lists of messages c, for all possible worlds $w \in W$ and for all formulae the following conditions are satisfied:

- $\langle \pi_i \parallel \lambda \rangle \psi \in flc(\varphi)$: if there exists a world $v \in W$ such that $w r_i v$ and $\psi \in t_v^c(\rho(v,c))$ then $\langle \pi_i \parallel \lambda \rangle \psi \in t_w^c(\rho(w,c))$;
- $\langle \mathtt{send}(m) \parallel \lambda \rangle \psi \in flc(\varphi)$: if $c' = (c_1, c_2 \star m)$ where $c = (c_1, c_2)$ and $\psi \in t_w^{c'}(\rho(w,c'))$ then $\langle \mathtt{send}(m) \parallel \lambda \rangle \psi \in t_w^c(\rho(w,c))$;
- $\langle \lambda \parallel \mathtt{send}(m) \rangle \psi \in flc(\varphi)$: if $c' = (c_1 \star m, c_2)$ where $c = (c_1, c_2)$ and $\psi \in t_w^{c'}(\rho(w,c'))$ then $\langle \lambda \parallel \mathtt{send}(m) \rangle \psi \in t_w^c(\rho(w,c))$;
- $\langle \mathtt{rec}(m) \parallel \lambda \rangle \psi \in flc(\varphi)$: if $c' = (c_1, c_2)$ where $c = (m \star c_1, c_2)$ and $\psi \in t_w^{c'}(\rho(w,c'))$ then $\langle \mathtt{rec}(m) \parallel \lambda \rangle \psi \in t_w^c(\rho(w,c))$;
- $\langle \lambda \parallel \mathtt{rec}(m) \rangle \psi \in flc(\varphi)$: if $c' = (c_1, c_2)$ where $c = (c_1, m \star c_2)$ and $\psi \in t_w^{c'}(\rho(w,c'))$ then $\langle \lambda \parallel \mathtt{rec}(m) \rangle \psi \in t_w^c(\rho(w,c))$.

In the previous definition the sign $\star$ denotes the concatenation of messages.

A run ρ is called *w-saturated* for $w \in W$, if for all lists of messages c and for all formulae the following conditions are satisfied:

- $\langle \pi_i \parallel \lambda \rangle \psi \in flc(\varphi)$: if $\langle \pi_i \parallel \lambda \rangle \psi \in t_w^c(\rho(w,c))$ then there exists a world $v \in W$ such that $w r_i v$ and $\psi \in t_v^c(\rho(v,c))$;
- $\langle \mathtt{send}(m) \parallel \lambda \rangle \psi \in flc(\varphi)$: if $\langle \mathtt{send}(m) \parallel \lambda \rangle \psi \in t_w^c(\rho(w,c))$ then $\psi \in t_w^{c'}(\rho(w,c'))$ where if $c = (c_1, c_2)$ then $c' = (c_1, c_2 \star m)$;
- $\langle \lambda \parallel \mathtt{send}(m) \rangle \psi \in flc(\varphi)$: if $\langle \lambda \parallel \mathtt{send}(m) \rangle \psi \in t_w^c(\rho(w,c))$ then $\psi \in t_w^{c'}(\rho(w,c'))$ where if $c = (c_1, c_2)$ then $c' = (c_1 \star m, c_2)$;
- $\langle \mathtt{rec}(m) \parallel \lambda \rangle \psi \in flc(\varphi)$: if $\langle \mathtt{rec}(m) \parallel \lambda \rangle \psi \in t_w^c(\rho(w,c))$ then $\psi \in t_w^{c'}(\rho(w,c'))$ where if $c = (m \star c_1, c_2)$ then $c' = (c_1, c_2)$;
- $\langle \lambda \parallel \mathtt{rec}(m) \rangle \psi \in flc(\varphi)$: if $\langle \lambda \parallel \mathtt{rec}(m) \rangle \psi \in t_w^c(\rho(w,c))$ then $\psi \in t_w^{c'}(\rho(w,c'))$ where if $c = (c_1, m \star c_2)$ then $c' = (c_1, c_2)$.

A run is *saturted*, if it is w-saturated for all $w \in W$. $\mathcal{Q} = (\mathcal{F}, q, \mathcal{R}, \lhd)$ is a *PDL$\times$PDL-quasimodel for* φ if $(\mathcal{F}, q)$ is a basic structure for φ of depth $m \leq md(\varphi)$ such that

(qm2) there exists a world $w_0 \in W$ and $\varphi \in t_{w_0}^{(\varepsilon,\varepsilon)}(x_0)$, where x_0 is the root of $\left(T_{w_0}^{(\varepsilon,\varepsilon)}, R_{w_0,1}^{(\varepsilon,\varepsilon)}, \ldots, R_{w_0,k}^{(\varepsilon,\varepsilon)}\right)$.

$\mathcal{R}$ is a set of coherent and saturated runs through $(\mathcal{F}, q)$ and $\lhd$ is a set of binary relation on $\mathcal{R}$ satisfying the following conditions:

(qm3) for all $\rho, \rho' \in \mathcal{R}$, if $\rho \lhd_i \rho'$ then $\rho(w,c) R_{w,i}^c \rho'(w,c)$ for all $w \in W$ and lists of messages c.

(qm4) $\mathcal{R}_0 \neq \varepsilon$ and for all $l < m$, $\rho \in \mathcal{R}_l$, $w \in W$, for all lists of messages c, $x \in T_w^c$, for all $1 \leq i \leq k$, if $\rho(w,c) R_{w,i}^c x$ then there is $\rho' \in \mathcal{R}_{l+1}$ such that $\rho'(w,c) = x$ and $\rho \lhd_i \rho'$.

Lemma 1. *An $\mathcal{ML}_2$ formula φ satisfiable in a product frame $\mathcal{F} \times \mathcal{G}$ iff there is a PDL×PDL-quasimodel for φ based on $\mathcal{F}$.*

Proof. Let $(\mathcal{F}, q, \mathcal{R}, \lhd)$ be a PDL×PDL-quasimodel for φ based on $\mathcal{F}$, where $\mathcal{F} = (W, r_1, \ldots, r_k)$. Take the product frame $\mathcal{F} \times (\mathcal{R}, \lhd)$, and define a valuation $\mathcal{V}$ in it as follows: $\mathcal{V}(p_i) = \{(w, \rho, c) | p \in t_w^c(\rho(w, c))\}$ for every propositional variable p_i. Let $\mathcal{M}$ be $(\mathcal{F} \times (\mathcal{R}, \lhd), \mathcal{V})$. By induction on the construction of $\psi \in flc(\varphi)$ we need to show that for every $(w, \rho, c) \in \mathcal{M}$ we have $(w, \rho, c) \models_{\mathcal{M}} \psi$ iff $\psi \in t_w^c(\rho(w, c))$.

- For variables this follows from the definition.
- For Booleans, types are Boolean saturated sets.
- $(w, \rho, c) \models_{\mathcal{M}} \langle \pi_i \,\|\, \lambda \rangle \psi$ (based on the definition of the semantics) iff there exists a world $w' \in W$ such that $w r_i w'$ and $(w', \rho, c) \models_{\mathcal{M}} \psi$. Then by induction hypothesis (IH) $\psi \in t_{w'}^c(\rho(w', c))$. ρ is saturated and coherent, so the previous holds iff $\langle \pi_i \,\|\, \lambda \rangle \psi \in t_w^c(\rho(w, c))$.
- $(w, \rho, c) \models_{\mathcal{M}} \langle \lambda \,\|\, \pi_i \rangle \psi$ (based on the definition of the semantics) iff there exists a run $\rho' \in \mathcal{R}$ such that $\rho \lhd_i \rho'$ and $(w, \rho', c) \models_{\mathcal{M}} \psi$. Then by IH $\psi \in t_w^c(\rho'(w, c))$. According to (qm3), from $\rho \lhd_i \rho'$ we get $\rho(w, c) R_{w,i}^c \rho'(w, c)$. Finally based on (qm1) we get that $\langle \lambda \,\|\, \pi_i \rangle \psi \in t_w^c(\rho(w, c))$.

  In other direction let assume, that $\langle \lambda \,\|\, \pi_i \rangle \psi \in t_w^c(\rho(w, c))$ Then by (qm1) there exists a $x \in T_w^c$ such that $\rho(w, c) R_i x$ and $\psi \in t_w^c(x)$. According to (qm4) there exists $\rho' \in \mathcal{R}$ such that $\rho \lhd_i \rho'$ and $\psi \in t_w^c(\rho'(w, c))$. By IH we get $(w, \rho', c) \models_{\mathcal{M}} \psi$ and finally according to the definition of the semantics $(w, \rho, c) \models_{\mathcal{M}} \langle \lambda \,\|\, \pi_i \rangle \psi$.
- $(w, \rho, c) \models_{\mathcal{M}} \langle \mathtt{send}(m) \,\|\, \lambda \rangle \psi$ iff $(w, \rho, c') \models_{\mathcal{M}} \psi$ where if $c = (c_1, c_2)$ then $c' = (c_1, c_2 \star m)$ (by def.). Then by IH $\psi \in t_w^{c'}(\rho(w, c'))$. ρ is saturated and coherent, so the previous holds iff $\langle \mathtt{send}(m) \,\|\, \lambda \rangle \psi \in t_w^c(\rho(w, c))$.
- $(w, \rho, c) \models_{\mathcal{M}} \langle \lambda \,\|\, \mathtt{send}(m) \rangle \psi$ iff $(w, \rho, c') \models_{\mathcal{M}} \psi$ where if $c = (c_1, c_2)$ then $c' = (c_1 \star m, c_2)$ (by def.). Then by IH $\psi \in t_w^{c'}(\rho(w, c'))$. ρ is saturated and coherent, so the previous holds iff $\langle \lambda \,\|\, \mathtt{send}(m) \rangle \psi \in t_w^c(\rho(w, c))$.
- $(w, \rho, c) \models_{\mathcal{M}} \langle \mathtt{rec}(m) \,\|\, \lambda \rangle \psi$ iff $(w, \rho, c') \models_{\mathcal{M}} \psi$ where if $c' = (c_1, c_2)$ then $c = (m \star c_1, c_2)$ (by def.). Then by IH $\psi \in t_w^{c'}(\rho(w, c'))$. ρ is saturated and coherent, so the previous holds iff $\langle \mathtt{rec}(m) \,\|\, \lambda \rangle \psi \in t_w^c(\rho(w, c))$.
- $(w, \rho, c) \models_{\mathcal{M}} \langle \lambda \,\|\, \mathtt{rec}(m) \rangle \psi$ iff $(w, \rho, c') \models_{\mathcal{M}} \psi$ where if $c' = (c_1, c_2)$ then $c = (c_1, m \star c_2)$ (by def.). Then by IH $\psi \in t_w^{c'}(\rho(w, c'))$. ρ is saturated and coherent, so the previous holds iff $\langle \lambda \,\|\, \mathtt{rec}(m) \rangle \psi \in t_w^c(\rho(w, c))$.

- $(w,\rho,c) \models_{\mathcal{M}} \langle \psi? \,\|\, \lambda\rangle\chi$ iff $(w,\rho,c) \models_{\mathcal{M}} \psi$ and $(w,\rho,c) \models_{\mathcal{M}} \chi$. By IH this is true iff $\psi \in t^c_w(\rho(w,c))$ and $\chi \in t^c_w(\rho(w,c))$. But according to (t7) this is true iff $\langle \psi? \,\|\, \lambda\rangle\chi \in t^c_w(\rho(w,c))$
- $(w,\rho,c) \models_{\mathcal{M}} \langle \lambda \,\|\, \psi?\rangle\chi$ iff $(w,\rho,c) \models_{\mathcal{M}} \psi$ and $(w,\rho,c) \models_{\mathcal{M}} \chi$. By IH this is true iff $\psi \in t^c_w(\rho(w,c))$ and $\chi \in t^c_w(\rho(w,c))$. But according to (t8) this is true iff $\langle \lambda \,\|\, \psi?\rangle\chi \in t^c_w(\rho(w,c))$
- $(w,\rho,c) \models_{\mathcal{M}} \langle \alpha(\alpha_1 \cup \alpha_2) \,\|\, \beta\rangle\psi$ iff $(w,\rho,c) \models_{\mathcal{M}} \langle \alpha(\alpha_1) \,\|\, \beta\rangle\psi$ or $(w,\rho,c) \models_{\mathcal{M}} \langle \alpha(\alpha_2) \,\|\, \beta\rangle\psi$ (by def.). By IH this is true iff $\langle \alpha(\alpha_1) \,\|\, \beta\rangle\psi \in t^c_w(\rho(w,c))$ or $\langle \alpha(\alpha_2) \,\|\, \beta\rangle\psi \in t^c_w\rho(w,c))$. But according to (t5) this is true iff $\langle \alpha(\alpha_1 \cup \alpha_2) \,\|\, \beta\rangle\psi \in t^c_w(\rho(w,c))$
- $(w,\rho,c) \models_{\mathcal{M}} \langle \alpha \,\|\, \beta(\beta_1 \cup \beta_2)\rangle\psi$ iff $(w,\rho,c) \models_{\mathcal{M}} \langle \alpha \,\|\, \beta(\beta_1)\rangle\psi$ or $(w,\rho,c) \models_{\mathcal{M}} \langle \alpha \,\|\, \beta(\beta_2)\rangle\psi$ (by def.). By IH this is true iff $\langle \alpha \,\|\, \beta(\beta_1)\rangle\psi \in t^c_w(\rho(w,c))$ or $\langle \alpha \,\|\, \beta(\beta_2)\rangle\psi \in t^c_w(\rho(w,c))$. But according to (t6) this is true iff $\langle \alpha \,\|\, \beta(\beta_1 \cup \beta_2)\rangle\psi \in t^c_w(\rho(w,c))$
- $(w,\rho,c) \models_{\mathcal{M}} \langle \pi_i; \alpha \,\|\, \lambda\rangle\psi$ iff there exitst a world w' such that $w r_i w'$ and $(w',\rho,c) \models_{\mathcal{M}} \langle \alpha \,\|\, \lambda\rangle\psi$ (by def.). Then by IH $\langle \alpha \,\|\, \lambda\rangle\psi \in t^c_{w'}(\rho(w',c))$. ρ is coherent and saturated, so $\langle \pi_i \,\|\, \lambda\rangle\langle \alpha \,\|\, \lambda\rangle\psi \in t^c_w(\rho(w,c))$. According to (t2) this is true iff $\langle \pi_i; \alpha \,\|\, \lambda\rangle\psi \in t^c_w(\rho(w,c))$.
- $(w,\rho,c) \models_{\mathcal{M}} \langle \lambda \,\|\, \pi_i; \beta\rangle\psi$ iff there exitst a run $\rho' \in \mathcal{R}$ such that $\rho \lhd_i \rho'$ and $(w,\rho',c) \models_{\mathcal{M}} \langle \lambda \,\|\, \beta\rangle\psi$ (by def.). Then by IH $\langle \lambda \,\|\, \beta\rangle\psi \in t^c_w(\rho'(w,c))$. According to (qm3) $\rho(w,c) R^c_{w,i} \rho'(w,c)$, and by (qm1) $\langle \lambda \,\|\, \pi_i\rangle\langle \lambda \,\|\, \beta\rangle\psi \in t^c_w(\rho(w,c))$. According to (t3) this is true iff $\langle \lambda \,\|\, \pi_i; \beta\rangle\psi \in t^c_w(\rho(w,c))$.
- $(w,\rho,c) \models_{\mathcal{M}} \langle \pi_i; \alpha \,\|\, \pi_j; \beta\rangle\psi$ iff $(w,\rho,c) \models_{\mathcal{M}} \langle \pi_i \,\|\, \lambda\rangle\langle \alpha \,\|\, \pi_j; \beta\rangle\psi$ or $(w,\rho,c) \models_{\mathcal{M}} \langle \lambda \,\|\, \pi_j\rangle\langle \pi_i; \alpha \,\|\, \beta\rangle\psi$. Based on previous points of this proof we get that $\langle \pi_i \,\|\, \lambda\rangle\langle \alpha \,\|\, \pi_j; \beta\rangle\psi \in t^c_w(\rho(w,c))$ or $\langle \lambda \,\|\, \pi_j\rangle\langle \pi_i; \alpha \,\|\, \beta\rangle\psi \in t^c_w(\rho(w,c))$. According to (t4) this is true iff $\langle \pi_i; \alpha \,\|\, \pi_j; \beta\rangle\psi \in t^c_w(\rho(w,c))$.

Therefore by (qm2), φ is satisfied in $\mathcal{M}$.

For the other direction, suppose that φ is satisfied in a model $\mathcal{M}$ based on the product $\mathcal{F} \times \mathcal{G}$ of frames $\mathcal{F} = (W, r_1, \ldots, r_k)$ and $\mathcal{G} = (\Delta, R_1, \ldots, R_k)$ By proposition 1.7 and 3.9 in [5] we may assume, that $\mathcal{G}$ is an intransitive tree of depth $m \leq md(\varphi)$ and $(w_0, x_0, (\varepsilon, \varepsilon)) \models_{\mathcal{M}} \varphi$ for some $w_0 \in W$ with x_0 being the root of $\mathcal{G}$. With every triple (w,x,c) where $w \in W$, $x \in \Delta$ and c is a lists of messages we associate the type $t(w,x,c) = \{\psi \in flc(\varphi) | (w,x,c) \models_{\mathcal{M}} \psi\}$.

Fix w and c and define a binary relation $\sim^c_w$ on Δ as follows:

- if x,$y \in \Delta$ of depth 0 then $x \sim^c_w y$ iff $t(w,x,c) = t(w,y,c)$.
- if x,$y \in \Delta$ of depth $l < md(\varphi)$ then $x \sim^c_w y$ iff $t(w,x,c) = t(w,y,c)$ and for all $z \in \Delta$ and for all $1 \leq i \leq k$

– if xR_iz then there exists a $z' \in \Delta$ such that yR_iz' and $z \sim^c_w z'$

– if yR_iz then there exists a $z' \in \Delta$ such that xR_iz' and $z \sim^c_w z'$.

Clearly $\sim^c_w$ is an equivalence relation on Δ. Denote by $[x]^c_w$ the $\sim^c_w$-equivalence class of x, and put $\Delta^c_w \leftrightharpoons \{[x]^c_w | x \in \Delta\}$, $s^c_w([x]^c_w) \leftrightharpoons t(w,x,c)$ and $[x]^c_w R^c_{w,i} [y]^c_w$ if there exists a $y' \in \Delta^c_w$ such that xR_iy'. Then by the definition of $\sim^c_w$, r^c_w is well-defined, and the structure $((\Delta^c_w, r^c_w), s^c_w)$ clearly satisfies (qm1'). The map $x \mapsto [x]^c_w$ is a p-morphism from (Δ, r_2) to (Δ^c_w, r^c_w), so it also satisfies (qm1). However (Δ^c_w, r^c_w) is not necessarily a tree.

The tree $(T^c_w, <^c_w)$ we need can be obtained from this structure:

$$T^c_w = \left\{ ([x_0]^c_w, \ldots, [x_l]^c_w) \middle| l \leq m,\ [x_0]^c_w r^c_{wi_1} [x_1]^c_w \cdots [x_{l-1}]^c_w r^c_{w,i_{l-1}} [x_l]^c_w \right\}$$

If $u, v \in T^c_w$ then $u <^c_{w,i} v$ iff $u = ([x_0]^c_w, \ldots, [x_l]^c_w)$, $v = ([x_0]^c_w, \ldots, [x_l]^c_w, [x_{l+1}]^c_w)$ and $x_lR_ix_{l+1}$. $t^c_w([x_0]^c_w, \ldots, [x_l]^c_w) \leftrightharpoons t(w,x,c)$. It is easy to show that $((T^c_w, <^c_w), t^c_w)$ is a quasistate for φ for any $w \in W$ and messages c. Moreover $\varphi \in t^{(\varepsilon,\varepsilon)}_{w_0}\left([x_0]^{(\varepsilon,\varepsilon)}_{w_0}\right)$. So by taking $q(w,c) \leftrightharpoons ((T^c_w, <^c_{w,1}, \ldots, <^c_{w,k}), t^c_w)$ for each $w \in W$ and each message c we obtain a basic structure $(\mathcal{F}, q)$ for φ statisfying (qm2). We need to define runs trough $(\mathcal{F}, q)$. To do this for each $l \leq m$ and each sequence $(x_0, \ldots, x_l)$ in Δ such that $x_0R_{i_1} \cdots R_{i_l}x_l$, take the map $\rho : (w,c) \mapsto ([x_0]^c_w, \ldots [x_0]^c_w)$. It is easy to check that ρ is a coherent and a saturated l-run. Let $\mathcal{R}$ be the set of all such runs. For ρ, $\rho' \in \mathcal{R}$ let $\rho \lhd_i \rho'$ iff $\rho(w,c) <^c_w \rho'(w,c)$ for all $w \in W$ and for all messages c. Then (qm3) holds by definition. It remains to prove (qm4). Let $\rho \in \mathcal{R}_l$, $v \in W$, c any messages and $z \in T^c_v$ be such that $\rho(v,c) <^c_v z$. We have to show that there is $\rho' \in \mathcal{R}_{l+1}$ such that $\rho \lhd_i \rho'$, and $\rho'(v,c) = z$. Since $\rho(v,c) <^c_{v,i} z$, we have $\rho(v,c) = ([x_0]^c_v, \ldots, [x_l]^c_v)$ and $z = ([x_0]^c_v, \ldots, [x_l]^c_v, [x_{l+1}]^c_v)$ for some $x_1, \ldots, x_l, x_{l+1}$ with $x_0R^c_{j_1}x_1 \cdots R^c_{j_l}x_l$ and $[x_l]^c_v r^c_{v,i} [x_{l+1}]^c_v$. By the definition of $R^c_{v,i}$ there is $y \in [x_{l+1}]^c_v$ such that x_lR_iy. But then the map $\rho' : (w,c) \mapsto ([x_0]^c_w, \ldots, [x_l]^c_w, [y]^c_w)$ is in $\mathcal{R}$. Thus $(\mathcal{F}, q, \mathcal{R}, \lhd)$ is a quasimodel for φ. □

4. Blocks

A block for φ with root w is quadruple $\mathcal{B} = (\mathcal{F}, q, \mathcal{R}, \lhd)$ such that

- $\mathcal{F} = (\Delta, <)$ is a tree of depth less equal 1 with root w
- $(\mathcal{F}, q)$ is a basic structure for φ of depth m for some $m < md(\varphi)$
- $\mathcal{R}$ is a set of coherent and saturated runs through $(\mathcal{F}, q)$
- $\lhd$ is a set of binary relation on $\mathcal{R}$ satisfying (qm3) and (qm4)

A set $\mathcal{S}$ of blocks for φ is called *satisfying*, if

- all blocks in $\mathcal{S}$ are of the same depth m for some $m < md(\varphi)$

- $\mathcal{S}$ contans a block satisfying (qm2), and
- for every block $\mathcal{B} = (\mathcal{F}, q, \mathcal{R}, \lhd)$ in $\mathcal{S}$ with $\mathcal{F} = (\Delta, <)$ and every $v \in \Delta$, and every messages c there exists a block $\mathcal{B}' = (\mathcal{F}', q', \mathcal{R}', \lhd')$ in $\mathcal{S}$ such that $q(v, c) = q'(w', c)$ for the root w' of $\mathcal{B}'$

Lemma 2. *There is a PDL×PDL-quasimodel for φ iff there is a satisfying set of blocks for φ such that the number of quasistates in each block does not exceed $M(\varphi) = 1 + (md(\varphi) + 1) \cdot p(\varphi) \cdot |\,flc(\varphi)|$.*

In the previous lemma $p(\varphi)$ is a finite constant depending on the φ. Its precise definition is in the first chapter of [5].

Proof. We call a quadruple $(\mathcal{F}, q, \mathcal{R}, \lhd)$ *a weak quasimodel for φ* if the following conditions hold:

(wq1) $\mathcal{F} = (W, r_1, \dots, r_k)$ is a finite frame and $(\mathcal{F}, q)$ is a basic structure for φ satisfying (qm2).

(wq2) $\mathcal{R}$ is a set of runs through $(\mathcal{F}, q)$ and $\lhd_i$ is a binary relation on $\mathcal{R}$, satisfying (qm3) and (qm4).

(wq3) for all messages c and for all w, $v \in W$ if $w \neq v$ and wr_iv then there exists a block $\mathcal{B}^c_{w,v} = (\mathcal{F}^c_{w,v}, q^c_{w,v}, \mathcal{R}^c_{w,v}, \lhd^c_{w,v})$ in $\mathcal{S}$ with $\mathcal{F}^c_{w,v} = (\Delta, <)$ such that
- $\Delta \subseteq W$, and w, $v \in \Delta$
- for all $u \in \Delta$, $q(u, c) = q^c_{w,v}(u, c)$
- for all u, $u' \in \Delta$ if ur_iu' then $u <_i u'$
- for all $\rho \in \mathcal{R}$ the restriction $\rho_{w,v}$ of ρ to Δ is a run in $\mathcal{R}^c_{w,v}$

Let $\mathcal{Q}_0 = (\mathcal{F}_0, q_0, \mathcal{R}_0, \lhd_0)$ be a block in $\mathcal{S}$ with root w_0 for which (qm2) holds. Now $\mathcal{Q}_0$ is a weak quasimodel. Suppose now that we have already constructed $\mathcal{Q}_n = (\mathcal{F}_n, q_n, \mathcal{R}_n, \lhd_n)$ with $\mathcal{F}_n = (W_n, r_{1n}, \dots r_{kn})$. For each $w \in W_n - W_{n-1}$ (where let $W_{-1} = w_0$) select a block $\mathcal{B}^c_w = (\mathcal{F}^c_w, q^c_w, \mathcal{R}^c_w, \lhd^c_w)$ from $\mathcal{S}$ with w as root and $\mathcal{F}^c_w = (\Delta^c_w, <^c_w)$ such that $q_n(w, c) = q^c_w(w, c)$. The existence of such block follows from (wq3). We may assume that all the selected blocks are pairwise disjoint and $\Delta^c_w \cap W_n = \{w\}$. Define $(\mathcal{F}_{n+1}, q_{n+1})$ by taking

$$W_{n+1} = W_n \cup \bigcup\{\Delta^c_w | w \in W_n - W_{n-1}\},$$
$$r_{n+1} = r_n \cup \bigcup\{<^c_w | w \in W_n - W_{n-1}\},$$
$$\mathcal{F}_{n+1} = (W_{n+1}, r_{n+1}),$$

$$q_{n+1}(v, c) = \begin{cases} q^c_w(v, c), & \text{if } v \in \Delta^c_w,\ w \in W_n - W_{n-1} \\ q_n(v, c), & \text{if } v \in W_n \end{cases}$$

Now let $\rho \in \mathcal{R}_n$ and $\bar{s} = \{s \in \mathcal{R}^c_w | w \in W_n - W_{n-1}$ and $s(w,c) = \rho(w,c)\}$ Define the extension $\rho \cup \bar{s}$ of ρ by taking for all $v \in W_{n+1}$

$$(\rho \cup \bar{s})(v,c) = \begin{cases} \rho^c_w(v,c), & \text{if } v \in \Delta^c_w,\ w \in W_n - W_{n-1} \\ \rho(v,c), & \text{if } v \in W_n \end{cases}$$

Let $\mathcal{R}_{n+1}$ be the set of all such extensions and let $(\rho_1 \cup \bar{s}_1) \lhd_{n+1,i} (\rho_2 \cup \bar{s}_2)$ iff $\rho_1 \lhd_{n,i} \rho_2$ and $s_1 \lhd^c_{w,i} s_2$ for all $w \in W_n - W_{n-1}$. It can be checked that $\mathcal{R}_{n+1}$ and $\lhd_n$ satisfy (qm3) and (qm4), and $\mathcal{Q}_{n+1} = (\mathcal{F}_{n+1}, q_{n+1}, \mathcal{R}_{n+1}, \lhd_{n+1})$ is a weak quasimodel. The *limit quasimodel* defined as follows. Let $\mathcal{F} = (W, r)$, where $W = \bigcup_n W_n$, $r = \bigcup_n r_n$ and let $q = \bigcup_n q_n$. For each sequence of $(\rho_0, \rho_1, \dots)$, where $\rho_n \in \mathcal{R}_n$ and ρ_{n+1} is an extension of ρ_n let $\rho = \bigcup_n \rho_n$. Let $\mathcal{R}$ is the set of all such runs. For ρ, $\rho' \in \mathcal{R}$ define $\rho \lhd_i \rho'$ iff $\rho \lhd_{n,i} \rho'$ for all n (where $\rho = \bigcup_n \rho'_n$).

We leave to the reader to show by using (wq1) and (wq3) that $(\mathcal{F}, q, \mathcal{R}, \lhd)$ is a quasimodel for φ. Here we show only that all runs in $\mathcal{R}$ are coherent and saturated, i.e. for all $\rho \in \mathcal{R}$, $w \in W$, for all messages c and formula $\langle \pi_i \parallel \lambda \rangle \psi \in flc(\varphi)$: $\langle \pi_i \parallel \lambda \rangle \psi \in t^c_w(\rho(w,c))$ iff there exists a world v such that wr_iv and $\psi \in t^c_v(\rho(v,c))$. Suppose that $\langle \pi_i \parallel \lambda \rangle \psi \in t^c_w(\rho(w,c))$ and let n such that $w \in W_n - W_{n-1}$. Then $\langle \pi_i \parallel \lambda \rangle \psi \in t^c_w(\rho_n(w,c))$, and by definition $\mathcal{Q}_{n+1}$ there exists $v \in W_{n+1}$ for which $wr_{n+1}v$ and $\psi \in t^c_v(\rho_{n+1}(v,c))$. Conversely, suppose wr_nv and $\psi \in t^c_v(\rho_n(v,c))$. Then it follows from (wq3) that $\langle \pi_i \parallel \lambda \rangle \psi \in t^c_w(\rho(w,c))$.

For the other direction of the proof, let us assume that we have a given quasimodel $\mathcal{Q} = (\mathcal{F}, q, \mathcal{R}, \lhd)$ for φ of depth $m \leq md(\varphi)$ with $\mathcal{F} = (W, r_1, \dots, r_k)$. Note first that we may assume each world w in $\mathcal{F}$ to have arbitrarily many indistinguishable copies in $\mathcal{Q}$ in the following sense. Say that two distinct worlds w, $w' \in W$ are *twins (in $\mathcal{Q}$)* if

- for all messages c, $q(w,c) = q(w',c)$
- for all $v \in W$, vr_iw iff vr_iw' and wr_iv iff $w'r_iv$,
- and for all runs $\rho \in \mathcal{R}$ and for all messages c, $\rho(w,c) = \rho(w',c)$.

To construct a satisfying set $\mathcal{S}$ of blocks, we will associate with each $w \in W$ and each messages c a block $\mathcal{B}^c_w = (\mathcal{F}^c_w, q^c_w, \mathcal{R}^c_w, \lhd^c_w)$ with w as root, such that $q^c_w(w,c) = q(w,c)$, and put $\mathcal{S} = \{\mathcal{B}\}$. The resulting $\mathcal{S}$ will clearly be a satisfying set of blocks for φ. Let $w \in W$ and c some lists of messages. First we define inductively sets of runs $\mathcal{P}_k \subseteq \mathcal{R}_k$, $k \leq m$:

- $\mathcal{P}_0 = \{\rho_0\}$

- Given $\mathcal{P}_k$, we construct $\mathcal{P}_{k+1}$ as follows. For every run $\rho \in \mathcal{P}_k$ and every $x \in T^c_w$ with $\rho(w,c) <^c_w x$, select an $\rho' \in \mathcal{R}_{k+1}$ such that $\rho \lhd \rho'$ and $\rho'(w,c) = x$, and put it into $\mathcal{P}_{k+1}$. Such a run exists by (qm4).

Finally let $\mathcal{P} = \bigcup_{l \leq m} \mathcal{P}_k$. For every $\rho \in \mathcal{P}$ and every $\langle \pi_i \parallel \lambda \rangle \psi \in t^c_w(\rho(w,c))$ we then let $Sat(\rho, c, \langle \pi_i \parallel \lambda \rangle \psi) = \{v \in W | wRv,\ \psi \in t^c_v(\rho(v,c))\}$. As ρ is saturated, $Sat(\rho, c, \langle \pi_i \parallel \lambda \rangle \psi) \neq \emptyset$. We select a finite subset $\Delta^c_w(\rho, \langle \pi_i \parallel \lambda \rangle \psi)$ of $Sat(\rho, c, \langle \pi_i \parallel \lambda \rangle \psi)$ in the following way. If $Sat(\rho, c, \langle \pi_i \parallel \lambda \rangle \psi) = \{w\}$, then $\Delta^c_w(\rho, \langle \pi_i \parallel \lambda \rangle \psi) = \{w\}$ as well. Otherwise let $\Delta^c_w(\rho, \langle \pi_i \parallel \lambda \rangle \psi)$ consist of a $v \neq w$ from $Sat(\rho, c, \langle \pi_i \parallel \lambda \rangle \psi)$ together with $m+1$ twins of v. We may assume that the obtained sets $\Delta^c_w(\rho, \langle \pi_i \parallel \lambda \rangle \psi)$ are pairwise disjoint. Now we define

- $\Delta^c_w = \{w\} \cup \bigcup \{\Delta^c_w(\rho, \langle \pi_i \parallel \lambda \rangle \psi) | \rho \in \mathcal{P},\ \langle \pi_i \parallel \lambda \rangle \psi \in t^c_w(\rho(w,c))\}$,
- for all v, $v' \in \Delta^c_w$, $v r^c_w v'$ iff $v = w$ and vRv',
- $\mathcal{F}^c_w = (\Delta^c_w, r^c_w)$ and
- for all $v \in \Delta^c_w$, $q^c_w = q(v)$.

Then $\mathcal{F}^c_w$ is a tree of depth ≤ 1 and $(\mathcal{F}^c_w, q^c_w)$ is a basic structure for φ. The cardinality of Δ^c_w is clearly bounded by $1 + (md(\varphi) + 1) \cdot p(\varphi) \cdot |\, flc(\varphi)|$.

It remains to define a set $\mathcal{R}^c_w$ of coherent and saturated runs through $(\mathcal{F}^c_w, q^c_w)$ and binary relations $\lhd^c_{w,i}$ on $\mathcal{R}^c_w$ such that (qm3) and (qm4) hold. Let $v \in \Delta^c_w$, $v \neq w$ and suppose that ρ and ρ' are functions whose domain contains Δ^c_w and $\rho(w,c) = \rho'(w,c)$. Define a function $\rho +_v \rho'$ with domain Δ^c_w by taking, for all $z \in \Delta^c_w$

$$(\rho +_v \rho')(z,c) = \begin{cases} \rho(z,c), & \text{if } z = v \\ \rho'(z,c), & \text{if } z \neq v. \end{cases}$$

Using this 'addition' function we now define sets $\mathcal{R}^c_{wl}$ of l-runs for every $l \leq m$. Let $\mathcal{R}^c_{w0}$ be the restriction of ρ_0 to Δ^c_w. For $k > 0$, we put all the restrictions of runs from $\mathcal{P}_l$ (to Δ^c_w) into $\mathcal{R}^c_{wl}$, and also add the functions $\rho_1 +_{v_1} (\rho_2 +_{v_2} (\dots (\rho_n +_{v_n} \rho) \dots))$, where $1 \leq n \leq l$, $\rho \in \mathcal{P}_l$, $\rho_1, \dots, \rho_n \in \mathcal{R}_l$ such that $\rho(w) = \rho_j(w)$, for $1 \leq j \leq n$, and $v_1, \dots, v_n$ are pairwise distinct points in Δ^c_w different from w.

Obviously every run $s \in \mathcal{R}^c_w$ is coherent. We show that it is w-saturated. This is clear if s is a restriction of some run from $\mathcal{P}$. Otherwise, s is on the form $\rho_1 +_{v_1} (\rho_2 +_{v_2} (\dots (\rho_n +_{v_n} \rho) \dots))$, for some $n \leq m$. So, we modified the w-saturated run ρ at most m places. Take some formula $\langle \pi_i \parallel \lambda \rangle \psi \in t^c_w(s(w,c))$. Since we selected for Δ^c_w $m+1$ twins for each point in $Sat(\rho, c, \langle \pi_i \parallel \lambda \rangle \psi)$, there is still at least one v left to 'saturate s with respect to $\langle \pi_i \parallel \lambda \rangle \psi$', that is such that $\psi \in t^c_v(s(v,c))$.

Finally let $s = \rho_1 +_{v_1} (\rho_2 +_{v_2} (\dots(\rho_n +_{v_n} \rho)\dots))$ and $s' = \rho'_1 +_{v'_1} (\rho'_2 +_{v'_2} (\dots(\rho'_l +_{v'_l} \rho')\dots))$ be two runs in $\mathcal{R}^c_w$. If s or s' is a restriction of some run from $\mathcal{P}$, then we consider n or l to be 0, respectively. We let $s \lhd^c_{w,i} s'$ if the following hold:

- $s \in \mathcal{R}^c_{w,l}$ and $s' \in \mathcal{R}^c_{w,l+1}$, for some $l < m$,
- $\rho \lhd_i \rho'$,
- $n \leq l$ and $v_j = v'_j$ for all $1 \leq j \leq n$,
- for all $z \in \Delta^c_w$, $\rho_j(z, c)\ r^c_{w,i}\ \rho'_j(z, c)$ whenever $1 \leq j \leq n$ and $\rho(z, c)\ r^c_{w,i}\ \rho'_j(z, c)$ whenever $n + 1 \leq j \leq l$.

Then (qm3) holds by definition. We show that (qm4) also holds. Suppose that $s = \rho_1 +_{v_1} (\rho_2 +_{v_2} (\dots(\rho_n +_{v_n} \rho)\dots))$, $z \in \Delta^c_w$, $x \in T^c_w$ and $s(z, c)R^c_{w,i}x$. We need a run $s' \in \mathcal{R}^c_w$ such that $s \lhd^c_{w,i} s'$ and $s'(z, c) = x$.
Case 1: $z = v_j$ for some $1 \leq j \leq n$. Then $s(z, c) = \rho_j(z, c) = v_j$ for some $\rho_j \in \mathcal{R}$. As the original quasimodel $\mathcal{Q}$ satisfies (qm4), we have a run $\rho'_j \in \mathcal{R}$ such that $\rho_j \lhd_i \rho'_j$ and $\rho'_j(z, c) = x$. Similarly for all $l \neq j$, $1 \leq l \leq n$, take a run ρ'_l from $\mathcal{R}$ such that $\rho_l \lhd_i \rho'_l$ and $\rho'_l(w, c) = \rho'_j(w, c)$. Finally take a run ρ' from $\mathcal{P}$ such that $\rho \lhd_i \rho'$ and $\rho'(w, c) = \rho'_j(w, c)$. Such a run exists by the definition of $\mathcal{P}$. Then $s' = \rho'_1 +_{v_1} (\rho'_2 +_{v_2} (\dots(\rho'_n +_{v_n} \rho')\dots))$ is a run in $\mathcal{R}^c_w$ as required.
Case 2: $z \neq v_j$ for any $1 \leq j \leq n$. Then $s(z, c) = \rho(z, c)$. Select a run ρ'_{n+1} from $\mathcal{R}$ such that $\rho \lhd_i \rho'_{n+1}$ and $\rho'_{n+1}(z, c) = x$. For each j, $1 \leq j \leq n$, take a run ρ'_j from $\mathcal{R}$ such that $\rho_j \lhd_i \rho'_j$ and $\rho'_j(w, c) = \rho'_{n+1}(w, c)$. Finally, take a run ρ' from $\mathcal{P}$ such that $\rho \lhd_i \rho'$ and $\rho'(w, c) = \rho'_{n+1}(w, c)$. Then $s' = \rho'_1 +_{v_1} (\rho'_2 +_{v_2} (\dots(\rho'_{n+1} +_z \rho')\dots))$ is a run in $\mathcal{R}^c_w$ as required.

Thus $(\mathcal{F}^c_w, q^c_w, \mathcal{R}^c_w, \lhd^c_w)$ is indeed a block with w as root. □

5. Conclusions

It has been shown that there is a quasimodel for φ iff there is exists a finite set S of finite blocks. The cardinality of S and the size of blocks are bounded by φ. From these blocks we are able to construct the quasimodel we need. This means that we are able to build up a finite construction for any formula φ of logic PDL×PDL. The number of this kind of finite constuctions is finite for any formulae, hence this logic is decidable.

References

[1] László Aszalós and Philippe Balbiani. Logical aspects of user authentication protocols. In *Proc. 7th Seminar RelMiCS, 2nd Workshop Kleene Algebra*, pages 277–287, Bad Malente, may 2003.

[2] László Aszalós and Philippe Balbiani. Some decidability result for logic constructed for checking user authentication protocols. *Journal of Computer Science and Control Systems*, 2008.

[3] Michael Burrows, Martín Abadi, and Roger Needham. A logic for authentication. In *Proceedings of the Royal Society of London*, volume 426, pages 233–271, 1989.

[4] John Clark and Jeremy Jacob. On the security of recent protocols. *Information Processing Letters*, 56:151–155, 1995.

[5] Dov M. Gabbay, Ágnes Kurucz, Frank Wolter, and Michael Zakharyaschev. *Many-Dimensional Modal Logics: Theory and Applications*. Studies in Logic and the Foundations of Mathematics. Elsevier, 2003.

[6] Dov M. Gabbay and Valentin B. Shehtman. Products of modal logics. I. *Logic Journal of the IGPL. Interest Group in Pure and Applied Logics*, 6(1):73–146, 1998.

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

[8] Ágnes Kurucz. S5 x s5 x s5 lacks the finite model property. In Frank Wolter, Heinrich Wansing, Maarten de Rijke, and Michael Zakharyaschev, editors, *Advances in Modal Logic*, pages 321–327. World Scientific, 2000.

[9] A. D. Rubin and P. Honeyman. Formal methods for the analysis of authentication protocols. Technical report, 1993.

Department of Computer Science, University of Debrecen; Institute de Recherche en Informatique de Toulouse

E-mail address: `aszalos@inf.unideb.hu, balbiani@irit.fr`