Razonando entre la lógica dinámica y la lógica lineal temporal usando álgebras de fork

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Tesistas

Juan Pablo Galeotti (jgaleotti@dc.uba.ar)
Mario Roman (mroman@dc.uba.ar)

Directores

Dr. Marcelo Frias (mfrias@dc.uba.ar)
Lic. Carlos Lopez Pombo (clpombo@dc.uba.ar)

2004

Resumen

La descripción de sistemas mediante distintas vistas es una práctica aceptada en la ingeniería de software moderna. En este trabajo, mostramos como es posible razonar en un marco relacional a través de especificaciones que capturan el comportamiento de un sistema. Para esto consideramos distintas vistas usando lógica lineal temporal, lógica dinámica o lógica dinámica lineal temporal. El principal resultado es que vistas generadas por separado pueden ser uniformazadas dentro de un marco relacional común al que pueden aplicarse distintas técnicas de análisis. Asimismo presentamos un problema del mundo real en el que probamos una propiedad no trivial de un sistema partiendo de las especificaciones de su comportamiento en lógica dinámica y en lógica lineal temporal.

Abstract

Describing systems through the specification of different views is a well accepted practice in modern software engineering. In this work we show how to reason across behavioral specifications within a relational framework. We consider views specifying behavioral information using linear temporal logic, dynamic logic or dynamic linear temporal logic. The main result is that independently generated specifications can be amalgamated within a common relational framework to which different analysis techniques can be applied. We also present a realistic problem for which behavioral specifications in dyamic logic and linear temporal logic are jointly employed in the proof of a non trivial property.

Agradecimientos de Juan Pablo Galeotti

Quiero agradecer a Charly y a Marcelo, por la enorme predisposición para explicarnos todo lo que quisimos aprender y el gran esfuerzo realizado para guiarnos durante todo este trabajo; y sobrellevar mi neurosis obsesiva.

A mis viejos, Adelma y Alberto, por su cariño, y a mi hermano Nicolás, por todo ;).

Agradecimientos de Mario Roman

Quiero agradecer a mi papá, a mi mamá y a mi hermana por el apoyo y el cariño brindado durante todos estos años de carrera, por aguantar mis malos humores, por hacerme feliz,

a mi Tía y a mis primas, por los recuerdos compartidos,

a mi novia, por el amor y la compañía que me dio en estos dos últimos años de mi vida,

a Laura 'Miano- Roman', por ser una más de la familia,

a Marcelo Frías, Carlos Lopez Pombo y Juan Pablo Galeotti, por permitirme compartir este trabajo con ellos,

a Badi, Cabeza, El Abuelo, El Beto, Gordo, Juan, Lacha, Negro, Nono, Pochi, Pogo, Rodro, Turco, Vaso, Venta, por ser mis amigos, y estar en los momentos más difíciles,

a Daniel Teira y Estaban Pavese , por esas divertidísimas tardes/noches de TPs, a Pablo Burzyn, Martin Urtasun, Alejo Caparelli, Matías Roth, Javier Altauz por todas esas tardes de estudio en la biblioteca del pabellón II,

a Diego Canteli, Lautaro Matas, Maxi Polimeni, por aceptarme como su amigo

a Mabel Bernis, por su ayuda,

y a todas aquellas personas que directa o indirectamente hayan contribuido en que este trabajo sea una realidad.

Por mi parte, esta tesis está dedicada a la única persona, que por esas cosas de la vida, no podrá darme un abrazo, un beso, o una felicitación.

Para una persona excelente,
para a un amigo increíble,
para a un ejemplo de vida,
para el gran ausente...
para vos viejo.

Contents

1 Introduction

The algebraization of logic consists on substituting reasoning (both at the logic and the metalogic level) by the study of properties of classes of algebras.

Fork Algebras [HV91] are an extension of relation algebras, and have been used towards the algebraization of classical and non-classical logics. Among the results that can be cited, we find the paper by Frias, Baum and Maibaum on the interpretability of first-order dynamic logic [FBM01], and the paper by Frias and Lopez Pombo on the interpretability of first-order linear temporal logics [FP]. These results constitute the foundations of the $\mathbf{A}r_{\mathbf{g}}$*entum* Project.

The $\mathbf{A}r_{\mathbf{g}}$*entum* project

$\mathbf{A}r_{\mathbf{g}}$*entum* is a CASE tool with relational foundations, under development at the laboratory of relational methods of the department of computer science at Universidad de Buenos Aires. Rather than using a single monolithic language for software specification, it uses different logics for modeling different views of systems. Thus, a system specification is a collection of theories coming from different logics. Using the interpretability results for these logics, the theories are translated to a uniform (regarding the language) relational specification. Once a relational specification is obtained, different tools such as model checkers or theorem provers can be applied in order to verify the relational specification.

For a graphical description of $\mathbf{A}r_{\mathbf{g}}$*entum*, see Fig. 1. The spheres located at the top of the figure stand for specifications of different views of a system according to different logics. The arrows originating at the spheres map logical specifications to a relational specification (located in the box targeted by the arrows). The homogeneous specification can later be analyzed using tools (the lower boxes) which can be plugged into $\mathbf{A}r_{\mathbf{g}}$*entum*.

Specifying system behavior

PDL [HKT00] is a formalism to reason about programs. It captures how system state evolve from program execution. On the other hand, LTL [Eme90] focuses on sequences of states, namely *execution paths*. In other words, LTL allows us to characterize those execution paths which are valid. In LTL, no notion of program arises.

Finally, DLTL [HT99] is an extension of LTL with the aim of adding dynamic flavor to a linear temporal logic. This logic allows us to express how a program "*consumes*" states along an execution path.

If we consider the union of PDL and LTL logics, then DLTL looks like the closest language to such formalism. Nevertheless, more expressive power leads to a more complicated deductive system, and requires the merging of clearly different concepts from both logics. These concepts are much closer to intuition when treated independently.

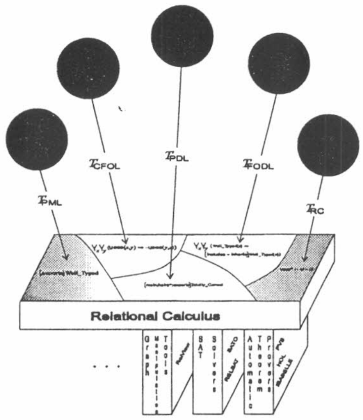

Figure 1: Architecture of $\mathbf{A}r_{\mathbf{g}}$*entum*

Goals

Given a system specification, different views of the system can be captured using PDL and LTL. In this work, we aim to use a relational calculus to homogenize these views, and verify properties that combines concepts from the dynamic view and the linear temporal view.

Notice that, since we regard PDL and LTL as *simple* logics, and DLTL as a *complex* one, this approach agrees with the $\mathbf{A}r_{\mathbf{g}}$*entum* project philosophy. Finally, we demonstrate its convenience with a study-case.

The work is organized as follows. In Section 2 we introduce the necessary mathematical basis for the remaining parts of the work. In sections 3, 4 and 5 we present mappings from PDL, LTL and DLTL formulas to relations in the calculus of the closure fork algebras. Also, in section 5, an interpretability theorem showing that any validity proof of an DLTL formula can be reduced to proving a certain equation in an equational calculus is proved. In section 6 we present an abstract framework of reasoning across PDL and LTL theories using the language of the fork algebras. In Section 7 a concrete case-study suitable for the abstract framework presented in 6 is given. Finally, in Section 8, we present the conclusions.

2 A Gentle Introduction to the Omega Closure Fork Algebras

In this section we will present the omega calculus for closure fork algebras (ω-CCFA) and its intended (standard) models, the omega closure fork algebras (ω-CFA), as they were defined in [BFM98].

In order to do so, we will begin in subsection 2.1 by defining a set of essential definitions and concepts. Later, in subsection 2.2 we will introduce the classes of algebras of binary relations and its abstract counterpart, the relational algebras, together with formalisms ETBR and CR. In subsection 2.3 we present fork algebras and finally, in subsection 2.4 we present the closure fork algebras (ω-CFA) and the *omega calculus for closure fork algebras* (ω-CCFA)).

2.1 A Introduction To Algebras

In this subsection we will present some fundamental definitions about algebras and some classes of algebras. It will be assumed that reader has a nodding acquaintance with elementary concepts of set-theory and first-order logic. As a reference text in both areas the reader is referred to [Bar77].

We begin by introducing what an algebra is. The interested reader is referred to [BS81].

Definition 2.1 *An algebra* $\mathfrak{A}$ *is a structure* $\langle A, f_1, \ldots, f_n \rangle$ *such that*

$$f_i : A^{arity(f_i)} \to A$$

for all $i \in [1, n]$.

Given an algebra $\mathfrak{A} = \langle A, f_1, \ldots, f_n \rangle$, A will be called the *universe* of $\mathfrak{A}$ and $f_1, \ldots f_n$ will be called the *operations* of $\mathfrak{A}$. If $arity(f_i) = 0$, f_i will be called a constant. The function $Rd : E \to E'$ takes reduct (some operations and sets of a given algebra are forgotten) of algebras of type E to the similarity type E'.

Definition 2.2 *Given two algebras* $\mathfrak{A} = \langle A, f_1, \ldots, f_n \rangle$ *and* $\mathfrak{B} = \langle B, g_1, \ldots, g_n \rangle$, $\mathfrak{B}$ *is a* subalgebra *of* $\mathfrak{A}$ *if*

- $B \subseteq A$
- $arity(f_i) = arity(g_i)$ *for all* i
- $f_i(b_1, \ldots, b_{arity(f_i)}) = g_i(b_1, \ldots, b_{arity(g_i)})$ *for all* $b_1, \ldots, b_{arity(g_i)} \in B$

Definition 2.3 *Let* $\mathfrak{A} = \langle A, f_1, \ldots, f_n \rangle$ *and* $\mathfrak{B} = \langle B, g_1, \ldots, g_n \rangle$ *two algebras such that arities match for each operation, a function* $h : A \to B$ *is an* homomorphism *from* $\mathfrak{A}$ *to* $\mathfrak{B}$ *if*

$$g_i(h(a_1), ..., h(a_{arity(g_i)})) = h(f_i(a_1, ..., a_{arity(f_i)}))$$

for all i.

$\mathfrak{B}$ is an *homomorphic image* of $\mathfrak{A}$ if exists such an homomorphism from $\mathfrak{A}$ to $\mathfrak{B}$. A bijective homomorphism is called *isomorphism*.

Definition 2.4 *Given an algebra $\mathfrak{A}$ and a class of algebras K, $\mathfrak{A}$ is* representable *in K if there exists $\mathfrak{B} \in K$ such that $\mathfrak{A}$ is isomorphic to $\mathfrak{B}$. This notion generalizes as follows: a class of algebras K_1 is representable in a class of algebras K_2 if every member of K_1 is representable in K_2.*

Definition 2.5 *An algebra $\mathfrak{A}$ with universe A is* simple *if:*

- $|A| \geq 2$

- *$\mathfrak{A}$ has exactly two homomorphic images*

Now, we present the class of boolean algebras.

Definition 2.6 *A* boolean algebra *is an algebra $\langle A, +, \cdot, {}^{-}, 0, \mathbf{1} \rangle$ where $+$ and $\cdot$ are binary operations, ${}^{-}$ is unary, and 0 and 1 are distinguished elements. The following identities are satisfied for all $x, y, z \in A$:*

$$\begin{aligned}
&\textit{idempotence}\begin{cases} x = & x \\ x\cdot x = & x \end{cases} \\
&\textit{commutativity}\begin{cases} x+y = & y+x \\ x\cdot y = & y\cdot x \end{cases} \\
&\textit{associativity}\begin{cases} x+(y+z) = (x+y)+z \\ x\cdot(y\cdot z) = (x\cdot y)\cdot z \end{cases} \\
&\textit{absorption}\begin{cases} x+(x\cdot y) = x \\ x\cdot(x+z) = x \end{cases} \\
&\textit{distributivity}\begin{cases} x\cdot(y+z) = & (x\cdot y)+(x\cdot z) \\ x+(y\cdot z) = & (x+y)\cdot(x+z) \end{cases} \\
&0 \textit{ and } \mathbf{1}\begin{cases} x\cdot 0 = & 0 \\ x+\mathbf{1} = & \mathbf{1} \end{cases} \\
&\textit{complement}\begin{cases} x\cdot\overline{x} = & 0 \\ x+\overline{x} = & 1 \end{cases}
\end{aligned}$$

2.2 Algebras of Binary Relations and the Calculus of Relations

In this subsection we will define the classes of algebras of binary relations and the class of relation algebras. The study of algebras of binary relations began with the works of Charles Sanders Peirce [Pei33] and Augustus De Morgan [dM66] and was later continued Ernst Schröder [Sch95] when looking for an algebraic counterpart of first-order reasoning, much the same as George Boole developed the so-called Boolean algebras as an algebraic counterpart to propositional reasoning.

Throughout the rest of this work, given a binary relation R in a set A, and $a, b \in A$, we will denote the fact that a and b are related via the relation R by $\langle a, b \rangle \in R$.

Definition 2.7 *Let E be a binary relation on a set A, and let R be a set of binary relations satisfying:*

- $\bigcup R \subseteq E$
- *Id is the identity relation on the set A and belongs to R*
- *$\emptyset$ is the empty relation and belongs to R*
- *E belongs to R*
- *R is closed under set union ($\cup$), intersection ($\cap$) and complement relative to E ($^-$)*
- *R is closed under relational composition (denoted by $\circ$) and converse (denoted by $\breve{}$). These two operations are defined by*

$$x \circ y = \{\langle a, c \rangle \,|\, (\exists b)(\langle a, b \rangle \in x \wedge \langle b, c \rangle \in y)\}$$

and

$$\breve{x} = \{\langle b, a \rangle \mid \langle a, b \rangle \in x\}$$

Then, the structure $\langle R, \cup, \cap, ^-, \emptyset, E, \circ, Id, \breve{}\, \rangle$ is called an algebra of binary relations.

The class of algebras of binary relations will be denoted as ABR, and the class of algebras of binary relations which are also simple algebras will be denoted by SimpleABR.

It follows from def. 2.7 that every algebra of binary relations has a boolean reduct.

In 1941 Alfred Tarski [Tar41] introduced the elementary theory of binary relations (ETBR) as a logical formalization of the algebras of binary relations. The elementary theory of binary relations is a formal theory with two different sorts. The set $IndVar = \{v_1, v_2, v_3, \dots\}$ contains the so-called *individual variables*, and the set $RelVar = \{R, S, T, \dots\}$ contains the so-called *relation variables*.

Definition 2.8 *The set of relation designations is the smallest set $RelDes$ such that:*

- $RelVar \cup \{0, \mathbf{1}, 1'\} \subseteq RelDes$
- *If $R, S \in RelDes$, then $\{\overline{R}, \breve{R}, R{+}S, R{\cdot}S, R;S\} \subseteq RelDes$*

Definition 2.9 *The set of atomic formulas of* ETBR *is the smallest set $AtomETBR$ satisfying:*

- $R = S \in AtomETBR$ *whenever* $R, S \in RelDes$
- $vRv' \in AtomETBR$ *whenever* $v, v' \in IndVar$ *and* $R \in RelDes$

From the atomic formulas, compound formulas are built as in first-order logic, with quantifiers applied only to individual variables. We will denote this set by $ForETBR$

Definition 2.10 *The set of formulas of* ETBR *is the smallest set* $ForETBR$ *satisfying:*

- $AtomETBR \subseteq ForETBR$
- *If* $\alpha, \beta \in ForETBR$ *and* $v \in IndVar$, *then* $\{\neg\alpha, \alpha \vee \beta, \exists v\ \alpha\} \subseteq ForETBR$

Definition 2.11 *We define the* ETBR *formalism as follows:*

- *Formulas:* $ForETBR$
- *Inference rules:*

$$\frac{\alpha \Longrightarrow \beta \qquad \alpha}{\beta} \quad (\textit{modus ponem})$$

$$\frac{\alpha}{\forall x\ \alpha} \quad (\textit{generalization})$$

- *Axioms:*

$\forall x \forall y (x \mathbf{1} y)$	(unit definition)
$\forall x \forall y (\neg x 0 y)$	(zero definition)
$\forall x (x 1' x)$	(reflexity of the identity)
$\forall x \forall y \forall z ((xRy \wedge y1'z) \Longrightarrow xRz)$	(identity is a congruence)
$\forall x \forall y (x\overline{R}y \Longleftrightarrow \neg xRz)$	(complement definition)
$\forall x \forall y (x\breve{R}y \Longleftrightarrow yRx)$	(converse definition)
$\forall x \forall y (xR{+}Sy \Longleftrightarrow xRy \vee xSy)$	(join definition)
$\forall x \forall y (xR{\cdot}Sy \Longleftrightarrow xRy \wedge xSy)$	(meet definition)
$\forall x \forall y (xR;Sy \Longleftrightarrow \exists z(xRz) \wedge (zSy))$	(relative product definition)
$R = S \Longleftrightarrow \forall x \forall y (xRy \Longleftrightarrow xSy)$	(equality definition)

Although the intended models of this theory were all the algebras of binary relations (ABR), Jónsson et al. in [JT52, Thm.4.10iii] proved that ETBR forces models to be simple (SimpleABR).

Definition 2.12 *Let* $\mathfrak{A} = \langle R, \cup, \cap, ^-, \emptyset, E, \circ, Id, ^\smile \rangle$ *be an algebra in* SimpleABR. *An* ETBR *model is a structure* $\langle \mathfrak{A}, m, v \rangle$ *where* m *is the meaning function that assigns relations in* R *to variables in* $RelVar$, *and* v *is the valuation function that assigns elements from* $B_{\mathfrak{A}}$ *to individual variables. It is clear how to extend* m *to a function* $m' : RelDes \to R$. *For the sake of simplicity, we will use the name* m *for both mappings.*

Definition 2.13 *Given an* ETBR *model* $\langle \mathfrak{A}, m, v\rangle$, *the semantics of a* ETBR *formula is defined recursively as follows:*

- $\langle \mathfrak{A}, m, v\rangle \models_{ETBR} xRy$ *iff* $\langle v(x), v(y)\rangle \in m(R)$
- $\langle \mathfrak{A}, m, v\rangle \models_{ETBR} R = S$ *iff* $m(R) = m(S)$
- $\langle \mathfrak{A}, m, v\rangle \models_{ETBR} \neg\alpha$ *iff* $\langle \mathfrak{A}, m, v\rangle \not\models_{ETBR} \alpha$
- $\langle \mathfrak{A}, m, v\rangle \models_{ETBR} \alpha \vee \beta$ *iff* $\langle \mathfrak{A}, m, v\rangle \models_{ETBR} \alpha$ *or* $\langle \mathfrak{A}, m, v\rangle \models_{ETBR} \beta$
- $\langle \mathfrak{A}, m, v\rangle \models_{ETBR} \exists x\, \alpha$ *iff exists* $a \in B_{\mathfrak{A}}$ *such that* $\langle \mathfrak{A}, m, v\rangle \models_{ETBR} \alpha[x/a]$

From the elementary theory of binary relations, Tarski [Tar41] introduced the *calculus of relations* (CR). The calculus of relations is defined as a restriction of the elementary theory of binary relations. Formulas of the calculus of relations are those formulas of the elementary theory of binary relations where no variables over individuals occur.

Definition 2.14 *The set of formulas of* CR *is the smallest set* $ForCR$ *satisfying:*

- $R = S \in ForCR$ *for all* $R, S \in RelDes$
- *If* $\alpha, \beta \in ForCR$, *then* $\{\neg\alpha, \alpha \vee \beta\} \subseteq ForCR$

As axioms of the calculus of relations, Tarski chose a subset of formulas without variables over individuals valid in the elementary theory of binary relations.

Definition 2.15 *We define* CR *formalism as follows:*

- *Formulas:* $ForCR$
- *Inference rules:*

$$\frac{}{R = R}$$

$$\frac{R = S}{S = R}$$

$$\frac{R = S \quad S = T}{R = T}$$

$$\frac{R_1 = S_1 \ \ldots \ R_k = S_k}{E(R_1, \ldots, R_k) = E(S_1, \ldots, S_k)}$$

- *Axioms:*

  1. $(R = S \wedge R = T) \Longrightarrow S = T$
  2. $R = S \Longrightarrow (R{+}T = S{+}T \wedge R{\cdot}T = S{\cdot}T)$
  3. $R{+}S = S{+}R \wedge R{\cdot}S = S{\cdot}R$
  4. $(R{+}S){\cdot}T = (R{\cdot}T){+}(S{\cdot}T) \wedge (R{\cdot}S){+}T = (R{+}T){\cdot}(S{+}T)$
  5. $R{+}0 = R \wedge R{\cdot}\mathbf{1} = R$

6. $R+\overline{R}=\mathbf{1} \wedge R\cdot\overline{R}=0$
7. $\overline{\mathbf{1}}=0$
8. $\breve{\breve{R}}=R$
9. $(R;S)^{\smile}=\breve{S};\breve{R}$
10. $(R;S);T=R;(S;T)$
11. $R;1'=R$
12. $(R;S)\cdot\breve{T}=0 \Longrightarrow (S;T)\cdot\breve{R}=0$
13. $R;\mathbf{1}=\mathbf{1} \vee \mathbf{1};\overline{R}=\mathbf{1}$

The semantics of CR is defined as a class of algebras.

Definition 2.16 *A* relation algebra *is an algebra* $\langle R,+,\cdot,^{-},0,\mathbf{1},;,1',^{\smile}\rangle$ *where* $+$, $\cdot$ *and* $;$ *are binary operations,* $^{-}$ *and* $^{\smile}$ *are unary operations, and* 0, $\mathbf{1}$ *and* $1'$ *are distinguished elements. Furthermore, the reduct* $\langle R,+,\cdot,^{-},0,\mathbf{1}\rangle$ *is a boolean algebra, and the following identities are satisfied for all* $x,y,z\in R$*:*

$$x;(y;z)=(x;y);z \tag{Ax. 1}$$

$$(x+y);z=x;z+y;z \tag{Ax. 2}$$

$$(x+y)^{\smile}=\breve{x}+\breve{y} \tag{Ax. 3}$$

$$\breve{\breve{x}}=x \tag{Ax. 4}$$

$$x;1'=1';x=x \tag{Ax. 5}$$

$$(x;y)^{\smile}=\breve{y};\breve{x} \tag{Ax. 6}$$

$$x;y\cdot z=0 \text{ iff } z;\breve{y}\cdot x=0 \text{ iff } \breve{x};z\cdot y=0 \tag{Ax. 7}$$

We will denote the class of all relation algebras by RA.

In [CT51] it was proved that formulas (1)-(12) can be proved from Axs. (1)-(7) and viceversa. If we add formula (13) to the axiomatization of relation algebras, we obtain the class of simple relation algebras (SimpleRA).

Definition 2.17 *Let* $\mathfrak{A}=\langle R,+,\cdot,^{-},0,\mathbf{1},;,1',^{\smile}\rangle$ *be an algebra in* SimpleRA. *A* CR *model is a structure* $\langle\mathfrak{A},m\rangle$ *where* m *is the meaning function that assigns relations in* R *to variables in* $RelVar$. *It is clear how to extend* m *to a function* $m':RelDes\to R$. *For the sake of simplicity, we will use the name* m *for both mappings.*

Definition 2.18 *Given an* CR *model* $\langle \mathfrak{A}, m \rangle$*, the semantics of a* CR *formula is defined recursively as follows:*

- $\langle \mathfrak{A}, m \rangle \models_{CR} R = S$ *iff* $m(R) = m(S)$
- $\langle \mathfrak{A}, m \rangle \models_{CR} \neg\alpha$ *iff* $\langle \mathfrak{A}, m \rangle \not\models_{CR} \alpha$
- $\langle \mathfrak{A}, m \rangle \models_{CR} \alpha \vee \beta$ *iff* $\langle \mathfrak{A}, m \rangle \models_{CR} \alpha$ *or* $\langle \mathfrak{A}, m \rangle \models_{CR} \beta$

Theorem 2.1 (See for instance [Fri02]) ABR $\subseteq$ RA

Theorem 2.2 ([Lyn50]) RA *is not representable in* ABR.

Theorem 2.3 ([Tar55]) *The class* RA *is a variety, i.e., it is axiomatizable with a set of equations.*

Theorem 2.4 ([TG87]) CR *is* equipollent*(equivalent) with a three variable fragment of first-order predicate logic.*

For the rest of this work, we will use the notation $x \leq y$ as a shorthand for the equation $x+y = y$.

Definition 2.19 *Let* $\mathfrak{A}$ *be a relation algebra.*

- *A relation* F *is called* functional *if* $\breve{F};F \leq 1'$.
- *A relation* I *is called* injective *if* $I;\breve{I} \leq 1'$.
- *A relation* S *is called* symmetric *if* $\breve{S} = S$.
- *A relation* T *is called* transitive *if* $T;T \leq T$.
- *A relation* D *is called* left-ideal *if* $D = \mathbf{1};D$.
- *A relation* D *is called* right-ideal *if* $D = D;\mathbf{1}$.
- *A relation* C *is* constant *if it is functional and* $C;\mathbf{1} = \mathbf{1}$.
- *By* $Dom(R)$ *we denote the relation* $(R;\breve{R})\cdot 1'$ *(the* domain *of relation* R*), and by* $Ran(R)$ *we denote the relation* $(\breve{R};R)\cdot 1'$ *(the* range *of the relation* R*).*

Given a binary relation R we denote by $\mathsf{dom}(R)$ and $\mathsf{ran}(R)$ the sets $\{x|(\exists y)(xRy)\}$ and $\{y|(\exists x)(xRy)\}$, respectively. Given a set S we denote its *power set* as $\mathcal{P}(S)$.

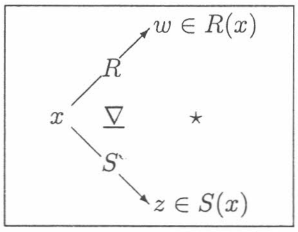

Figure 2: The operator fork.

2.3 Proper Fork Algebras and the Calculus of Fork Relations

If we are looking for a framework suitable for system specification, two important drawbacks arise from using CR. First, as a consequence of Thm. 2.2, some models of CR cannot be *seen* as any algebra of binary relations. This means that CR lacks of relational semantics (i.e. the universe of the algebra is not a set of binary relations). Secondly, and perhaps more harmful, because of Thm. 2.4, we will not be able to *import* specifications written in first-order predicate logic with more than three variables.

Nevertheless, an advantage for using CR is its deductive system. It is quite simple due to an equational finite axiomatization (which follows from Thm. 2.3) and simpler inference rules.

Fork algebras were introduced by Haeberer and Veloso [HV91] when looking for a formalism such that it overcomes the latter drawbacks and preserves CR simple deductive system.

Definition 2.20 *A* pre proper fork algebra *is a two-sorted algebraic structure* $\langle R, U, \cup, \cap, ^{-}, \emptyset, E, \circ, Id, \breve{}, \underline{\nabla}, \star\rangle$ *with domains R and U, such that:*

- $\langle R, \cup, \cap, ^{-}, \emptyset, E, \circ, Id, \breve{}\rangle$ *is an algebra of binary relations on the set U*
- $\star : U \times U \to U$ *is a binary function that is injective on the restriction of its domain to E*
- *R is closed under fork of binary relations, defined by:*

$$S \underline{\nabla} T = \{\langle x, \star(y, z)\rangle \,|xSy \wedge xTz\}$$

We will denote the class of pre proper fork algebras as PrePFA.

The definition of $\underline{\nabla}$ is depicted in Fig. 2. Whenever x and y are related via R, and x and z are related via S, x and $\star(y, z)$ are related via $R\underline{\nabla}S$.

Definition 2.21 *We define the class of proper fork algebras (denoted by* PFA*) as* **Rd**PrePFA*, where the operation* **Rd** *takes reducts to the similarity type* $\langle R, \cup, \cap, ^{-}, \emptyset, E, \circ, Id, \breve{}, \underline{\nabla}\rangle$.

We denote the class of proper fork algebras that are also simple algebras as SimplePFA.

It was in [FBHV95] where the class of proper fork algebras as previously depicted came up. From the first definition of fork algebras ([HV91]) until the latter work, the definition of fork evolved around the definition of the function $\star$.

The only requirement placed on function $\star$ by Frias et al. was that it had to be injective. This was enough to prove in [FHV97] that the newly defined class of fork algebras was indeed finitely axiomatizable by a set of equations.

In a similar way as Tarski, we will define the elementary theory of fork relations (ETFR for short) having as target the definition of the class PFA. As in ETBR, $IndVar$ contains the individual variables and $RelVar$ contains the relation variables.

Definition 2.22 *The set of* relation designations *of* ETFR *is the smallest set* $ForkRelDes$ *satisfying:*

- $RelDes \subseteq ForkRelDes$
- *If* $R, S \in ForkRelDes$, *then* $R\nabla S \in ForkRelDes$

Definition 2.23 *The set of individual terms of* ETFR *is the smallest set* $ForkIndTerm$ *satisfying:*

- $IndVar \subseteq ForkIndTerm$
- $t_1, t_2 \in ForkIndTerm$, *then* $\star(t_1, t_2) \in ForkIndTerm$

Definition 2.24 *The set of atomic formulas of* ETFR *is the smallest set* $AtomForkFor$ *satisfying:*

- *If* $R, S \in ForkRelDes$, *then* $R = S \in AtomForkFor$
- *If* $t_1, t_2 \in ForkIndTerm$ *and* $R \in ForkRelDes$, *then* $t_1 R t_2 \in AtomForkFor$

Definition 2.25 *The set of formulas of* ETFR *is the smallest set* $ForETFR$ *satisfying:*

- $AtomForkFor \subseteq ForETFR$
- *If* $\alpha, \beta \in ForETFR$ *and* $x \in IndVar$, *then* $\{\neg\alpha, \alpha\vee\beta, \exists x\alpha\} \subseteq ForETFR$

Definition 2.26 *We define the* ETFR *formalism as follows:*

- *Formulas:* $ForETFR$
- *Inference rules: the same as* ETBR
- *Axioms: Extend the axioms of* ETBR *by adding*
  1. $\forall x \forall y (xR\nabla Sy) \iff \exists u \exists v (y = \star(u, v) \wedge xRu \wedge xSv))$

2. $\forall x \forall y \forall u \forall v (\star(x,y) = \star(u,v) \Longrightarrow x = u \wedge y = v)$

Definition 2.27 *Let* $\mathfrak{A} = \langle R, \cup, \cap, ^-, \emptyset, E, \circ, Id, ^{\smile}, \underline{\nabla} \rangle$ *be an algebra in* SimplePFA. *An* ETFR *model is a structure* $\langle \mathfrak{A}, m, v \rangle$ *where* m *is the meaning function that assigns relations in* R *to variables in* $RelVar$, *and* v *is the valuation function that assigns elements from* $B_{\mathfrak{A}}$ *to individual variables. It is clear how to extend* m *to a function* $m' : RelDes \rightarrow R$ *and* v *to a function* $v' : ForkIndTerm \rightarrow B_{\mathfrak{A}}$. *For the sake of simplicity, we will use the name* m *and* v *for both mappings.*

Definition 2.28 *Given an* ETFR *model* $\langle \mathfrak{A}, m, v \rangle$, *the semantics of a* ETFR *formula is defined recursively as follows:*

- $\langle \mathfrak{A}, m, v \rangle \models_{ETFR} t_1 R t_2$ *iff* $\langle v(t_1), v(t_2) \rangle \in m(R)$
- $\langle \mathfrak{A}, m, v \rangle \models_{ETFR} R = S$ *iff* $m(R) = m(S)$
- $\langle \mathfrak{A}, m, v \rangle \models_{ETFR} \neg\alpha$ *iff* $\langle \mathfrak{A}, m, v \rangle \not\models_{ETFR} \alpha$
- $\langle \mathfrak{A}, m, v \rangle \models_{ETFR} \alpha \vee \beta$ *iff* $\langle \mathfrak{A}, m, v \rangle \models_{ETFR} \alpha$ *or* $\langle \mathfrak{A}, m, v \rangle \models_{ETFR} \beta$
- $\langle \mathfrak{A}, m, v \rangle \models_{ETFR} \exists x\ \alpha$ *iff there exists* $a \in B_{\mathfrak{A}}$ *such that* $\langle \mathfrak{A}, m, v \rangle \models_{ETFR} \alpha[x/a]$

Much the same as relation algebras are an abstract version of algebras of binary relations, proper fork algebras also have their abstract counterpart.

Definition 2.29 *An* abstract fork algebra *is a structure* $\langle R, +, \cdot, ^-, 0, \mathbf{1}, ;, 1', ^{\smile}, \nabla \rangle$ *where* $\langle R, +, \cdot, ^-, 0, \mathbf{1}, ;, 1', ^{\smile} \rangle$ *is a relation algebra and for all* $r, s, t, q \in R$,

$$r \nabla s = (r; (1' \nabla \mathbf{1})) \cdot (s; (\mathbf{1} \nabla 1')) \qquad \text{(Ax. 8)}$$

$$(r \nabla s); (t \nabla q)^{\smile} = (r; \breve{t}) \cdot (s; \breve{q}) \qquad \text{(Ax. 9)}$$

$$(1' \nabla \mathbf{1})^{\smile} \nabla (\mathbf{1} \nabla 1')^{\smile} \leq 1' \qquad \text{(Ax. 10)}$$

We denote the class of abstract fork algebras as AFA. Due to the definition, this class can be axiomatized with a finite set of equations. We denote the class of abstract fork algebras that are also simple algebras as SimpleAFA.

In a similar way as Tarski defined his calculus of relations, Veloso et al. defined a calculus of fork relations (CFR) from the elementary theory of fork relations.

Definition 2.30 *We define the formalism* CFR *as follows:*

- *Fromulas: Those formulas from* ETFR *in which there is no occurrence of the individual variables. The set of formulas of* CFR *will be denoted* $ForCFR$
- *Inference rules: Same as* ETBR

- *Axioms: Extend the axioms of* CR *by adding Axs. (8)-(10).*

Definition 2.31 *Let* $\mathfrak{A} = \langle R, +, \cdot, ^{-}, 0, \mathbf{1}, ;, 1', ^{\smile}, \nabla \rangle$ *be an algebra in* SimpleAFA. *A* CFR *model is a structure* $\langle \mathfrak{A}, m \rangle$ *where* m *is the meaning function that assigns relations in* R *to variables in* $RelVar$. *It is clear how to extend* m *to a function* $m' : RelDes \to R$. *For the sake of simplicity, we will use the name* m *for both mappings.*

Definition 2.32 *Given an* CFR *model* $\langle \mathfrak{A}, m \rangle$, *the semantics of a* CFR *formula is defined recursively as follows:*

- $\langle \mathfrak{A}, m \rangle \models_{CFR} R = S$ *iff* $m(R) = m(S)$
- $\langle \mathfrak{A}, m \rangle \models_{CFR} \neg\alpha$ *iff* $\langle \mathfrak{A}, m \rangle \not\models_{CFR} \alpha$
- $\langle \mathfrak{A}, m \rangle \models_{CFR} \alpha \vee \beta$ *iff* $\langle \mathfrak{A}, m \rangle \models_{CFR} \alpha$ *or* $\langle \mathfrak{A}, m \rangle \models_{CFR} \beta$

Once defined both formalisms (ETFR and CFR) and their target classes (PFA and AFA), we present the following theorems to determine the relationship between both classes.

Theorem 2.5 ([Fri02]) PFA $\subseteq$ AFA

Theorem 2.6 ([FHV97, Gyu97]) AFA *is representable in* PFA

Since every proper fork algebra is an abstract fork algebra, and every abstract fork algebra is isomorphic to a proper fork algebra, the relational semantics of all models of CFR is assured.

Finally, in [VHF95], interpretability of *FOLE* in CFR through a semantic preserving translation was proved. Hence, we are able to *import FOLE* specifications into CFR.

We suggest the reader to take a look at [Fri02, Ch. 2] for another equally valid semantic preserving translation and interpretability proof.

Given a $\mathfrak{A} \in$ PFA, elements from the base that do not represent pairs will be called *urelements*. The set of urelements from $\mathfrak{A}$ will be denoted by $Urel_{\mathfrak{A}}$.

The next lemma proves that, given a proper fork algebra, it is possible to single out its urelements (if there are any).

Lemma 2.1 *Let* $\mathfrak{A} \in$ PFA

$$Urel_{\mathfrak{A}} = \mathsf{dom}\left(Ran\left(\overline{\mathbf{1}\nabla\mathbf{1}}\right)\right)$$

Proof. It follows from the def. of PFA and dom. ■

We will denote the CFR term $Ran\left(\overline{\mathbf{1}\nabla\mathbf{1}}\right)$ by $1'_{\mathsf{U}}$. Notice that in the previous definitions we used AFA operations when referring to PFA operations. Since PFA $\subseteq$ AFA, it is clear how such mapping is defined.

Under the previous definitions, the equation

$$\mathbf{1} ; 1'_{\mathsf{U}} ; \mathbf{1} = \mathbf{1}$$

is valid in a proper fork algebra $\mathfrak{A}$ if and only if $Urel_{\mathfrak{A}}$ is not an empty set. We denote by PFAU the class of proper fork algebras with urelements and by AFAU the class of abstract fork algebras with urelements.

When interpreted in proper fork algebras, the relations $(1' \nabla \mathbf{1})^{\smile}$ and $(\mathbf{1} \nabla 1')^{\smile}$ behave as projections, projecting components from pairs constructed by applying $\star$ to two elements in the universe. As is usual in literature, we call them π and ρ respectively. They will allow us to cope with the lack of variables over individuals in CFR. Figure 3 illustrates the meaning of these relations.

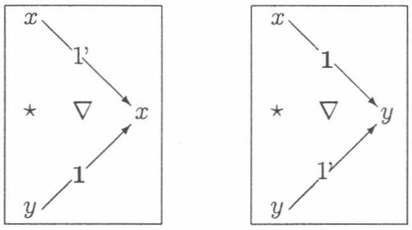

Figure 3: The projections π and ρ.

The operation *cross* (denoted by $\otimes$) performs a kind of parallel product. A graphic representation of cross is given in Fig. 4. An ETFR definition is given by

$$\forall w \forall x \forall y \forall z (\star(w, x) R \otimes S \star (y, z) \iff wRy \wedge xSz)$$

Under the definitions of π and ρ, the latter formula can be expressed in CFR as follows:

$$R \otimes S = (\pi ; R) \nabla (\rho ; S)$$

It is not difficult to check that both definitions are equivalent. The proof is left as an exercise to the eager reader.

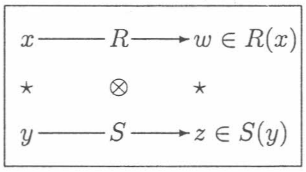

Figure 4: The operator cross.

2.4 Proper Closure Fork Algebras and the ω-Calculus of Closure Fork Relations

In [BFM98] the class of PCFA is introduced, and the omega calculus for closure fork algebras (ω-CCFA) was defined.

Definition 2.33 *We define the i-th folded composition of a relation R (denoted as $R^{;i}$) by the conditions:*

$$\begin{aligned} R^{;0} &= 1' \\ R^{(;n+1)} &= R;R^{;n} \end{aligned}$$

Definition 2.34 *Let $\langle R, U, \cup, \cap, ^{-}, \emptyset, E, \circ, Id, ^{\smile}, \underline{\nabla}, \star \rangle$ be a pre proper fork algebra, and let $^{\diamond}$ and * unary functions from R to R, satisfying:*

- *R is closed under R^{*}, the reflexive-transitive closure defined by*

$$R^{*} = \bigcup_{i \geq 0} R^{;i}$$

- *R is closed under $R^{\diamond}$, the set choice operator defined by condition*

$$x^{\diamond} \subseteq x \wedge |x^{\diamond}| = 1 \Longleftrightarrow x \neq \emptyset$$

Then, the structure $\langle R, U, \cup, \cap, ^{-}, \emptyset, E, \circ, Id, ^{\smile}, \underline{\nabla}, \star, ^{\diamond}, ^{*} \rangle$ is a pre proper closure fork algebra.

We denote the class of pre proper closure fork algebras by PrePCFA.

Definition 2.35 *We define the class* PCFA *as* **Rd**PrePCFA *where* **Rd** *takes reducts to structures of the form*

$$\langle R, \cup, \cap, ^{-}, \emptyset, E, \circ, Id, ^{\smile}, \underline{\nabla}, ^{\diamond}, ^{*} \rangle$$

Definition 2.36 *A* closure fork algebra *is a structure of the form*

$$\langle R, +, \cdot, ^{-}, 0, \mathbf{1}, ;, 1', ^{\smile}, \nabla, ^{\diamond}, ^{*} \rangle$$

where $\langle R, +, \cdot, ^{-}, 0, \mathbf{1}, ;, 1', ^{\smile}, \nabla \rangle$ is an abstract fork algebra and for all $x, y \in R$,

$$x^{\diamond};\mathbf{1};\breve{x^{\diamond}} \leq 1' \qquad (Ax.\ 11)$$

$$\breve{x^{\diamond}};\mathbf{1};x^{\diamond} \leq 1' \qquad (Ax.\ 12)$$

$$\mathbf{1};(x \cdot x^{\diamond});\mathbf{1} = \mathbf{1};x;\mathbf{1} \qquad (Ax.\ 13)$$

$$x^{*} = 1' + x;x^{*} \qquad (Ax.\ 14)$$

$$x^{*};y \leq y + x^{*};(\overline{y} \cdot x;y) \qquad (Ax.\ 15)$$

In the following paragraphs we introduce the *calculus for closure fork algebras* (CCFA)

Definition 2.37 *The set of relation designations of* CCFA *is the smallest set* $ClosureForkRelDes$ *satisfying:*

- $ForkRelDes \subseteq ClosureForkRelDes$
- *If* $x \in ClosureForkRelDes$, *then* $\{x^*, x^\circ\} \subseteq ClosureForkRelDes$

Definition 2.38 *Given a set of relation variables* $RelVar$, *the set of* CCFA *formulas on* $RelVar$ *is the set of identities* $t_1 = t_2$, *with* $t_1, t_2 \in ClosureForkRelDes$ *and it is denoted by* $ForCCFA$.

Definition 2.39 *We define the formalism* CCFA *as follows:*

- *Formulas:* $ForCCFA$
- *Inference rules: Same as* CFR
- *Axioms: Extend the axioms of* CFR *by adding Axs. (11)-(15).*

Definition 2.40 *We define the calculus* ω-CCFA *as the extension of the* CCFA *obtained by adding the following inference rule:*

$$\frac{\vdash 1' \leq y \qquad x^i \leq y \vdash x^{i+1} \leq y}{\vdash x^* \leq y} \qquad (i \in I\!N)$$

Definition 2.41 *We define the class of* omega closure fork algebras *(*ω-CFA*) as the models of the identities provable in* ω-CCFA.

Notice that every member of ω-CFA has a simple abstract fork algebra reduct.

Theorem 2.7 ([FBM01]) PCFA $\subseteq \omega$-CFA

Theorem 2.8 ([FBM01]) ω-CFA *is representable in* PCFA

Definition 2.42 *Let* $\mathfrak{A} = \langle R, +, \cdot, ^-, 0, \mathbf{1}, ;, 1', ^\smile, \nabla, ^\circ, ^* \rangle$ *be an algebra in* ω-CFA. *A* ω-CCFA *model is a structure* $\langle \mathfrak{A}, m \rangle$ *where* m *be a meaning function* $m : RelVar \to R$ *that assigns relations in* R *to variables in* $RelVar$. *It is clear how to extend* m *to a function* $m' : ClosureForkRelDes \to R$. *As previously done with the definitions of* CR *models and* CFR *models, we will use the name* m *for both functions.*

Definition 2.43 *Let* $\langle \mathfrak{A}, m \rangle$ *be an* ω-CCFA *model, the semantics of a* ω-CCFA *formula* α *is defined as follows:*

- $\mathfrak{A}, m \models_{\omega\text{-CCFA}} R = S$ *iff* $m(R) = m(S)$
- $\mathfrak{A}, m \models_{\omega\text{-CCFA}} \neg\beta$ *iff* $\mathfrak{A}, m \not\models_{\omega\text{-CCFA}} \beta$
- $\mathfrak{A}, m \models_{\omega\text{-CCFA}} \beta \vee \gamma$ *iff* $\mathfrak{A}, m \models_{\omega\text{-CCFA}} \beta$ *or* $\mathfrak{A}, m \models_{\omega\text{-CCFA}} \gamma$

Theorem 2.9 ([FBM01, Thm. 8]) *Let* α *be a* ω-CCFA *equation. Then,*

$$\models_{\omega\text{-CCFA}} \alpha \iff \vdash_{\omega\text{-CCFA}} \alpha$$

3 Interpreting PDL in Fork Algebras

The syntax and semantics of propositional dynamic logic (PDL) can be found in [HKT00]. PDL is a formalism for reasoning about programs. From a set of atomic actions, and using combinators, it is possible to build more complex programs. PDL is a modal logic where the behavior of the modal operators is determined by programs, understood as binary relations among on a set of computational states.

When compared to classical propositional logic, the difference is the dynamic content, which is clear in the notion of satisfiability. While satisfiability in classical propositional logic depends on a single valuation, in PDL there is a multiplicity of valuations, in which valuation we evaluate will depend on the state the program has reached.

Along this work we will assume a fixed (but arbitrary) finite signature $\Sigma = \langle A, P \rangle$ where $A = \{a_i\}_{i \in \mathcal{A}}$ are the atomic action symbols, and $P = \{p_i\}_{i \in \mathcal{P}}$ are the atomic proposition symbols.

Definition 3.1 *The set of programs and formulas on* Σ *are the smallest sets* $PrgPDL(\Sigma)$ *and* $ForPDL(\Sigma)$ *satisfying:*

- $A \subseteq PrgPDL(\Sigma)$
- *If* $\{r, s\} \subseteq PrgPDL(\Sigma)$*, then* $\{r;s, r \cup s, r^*\} \subseteq PrgPDL(\Sigma)$
- *If* $\alpha \in ForPDL(\Sigma)$*, then* $\alpha? \in PrgPDL(\Sigma)$
- $P \subseteq ForPDL(\Sigma)$
- *If* $\{\alpha, \beta\} \subseteq ForPDL(\Sigma)$*, then* $\{\neg\alpha, \alpha \vee \beta\} \subseteq ForPDL(\Sigma)$
- *If* $\alpha \in ForPDL(\Sigma)$ *and* $r \in PrgPDL(\Sigma)$*, then* $\langle r \rangle \alpha \in ForPDL(\Sigma)$

The semantics of PDL formulas is defined over a Kripke structure K of the form $\langle S, \tilde{A}, \tilde{P} \rangle$, where S is a set of states, $\tilde{A} = \{\tilde{a_i}\}_{i \in \mathcal{A}}$ is a set of binary relations on S and $\tilde{P} = \{\tilde{p_i}\}_{i \in \mathcal{P}}$ is a set where $\tilde{p_i} \subseteq S$ for all $i \in \mathcal{P}$.

Given a Kripke structure K and a signature Σ, we can map A to $\tilde{A}$ and P to $\tilde{P}$ using the subindexes.

Definition 3.2 *Given a K Kripke structure for the signature* Σ *and* $q \in S_K$*, the semantics of a PDL formula is defined recursively as follows:*

- $K, q \models_{PDL} p_i$ *iff* $q \in \tilde{p_i}$
- $K, q \models_{PDL} \neg\alpha$ *iff* $K, q \not\models_{PDL} \alpha$
- $K, q \models_{PDL} \alpha \vee \beta$ *iff* $K, q \models_{PDL} \alpha$ *or* $K, q \models_{PDL} \beta$
- $K, q \models_{PDL} \langle r \rangle \alpha$ *iff exists* $q' \in S_K$ *such that* $\langle q, q' \rangle \in Prg_K(r)$ *and* $K, q' \models_{PDL} \alpha$
- $Prg_K(a_i) = \tilde{a_i}$

- $Prg_K(r;s) = Prg_K(r);Prg_K(s)$
- $Prg_K(r \cup s) = Prg_K(r) \cup Prg_K(s)$
- $Prg_K(r^*) = (Prg_K(r))^*$
- $Prg_K(\alpha?) = \{\langle q, q\rangle \,|K, q \models_{PDL} \alpha\}$

A formula $\alpha \in ForPDL(\Sigma)$ is satisfied in a Kripke structure K for Σ if there exists a state $q \in S_K$ such that $K, q \models_{PDL} \alpha$. A formula is valid in a Kripke structure K if it is satisfied for all $q \in S_K$.

In [FO98], Frias and Orlowska presented an interpretability result for PDL in ω-closure calculus of fork algebras. We present their result in this section.

Defining the translation for a dynamic language with signature Σ, requires extending the language of ω-closure fork algebras with new constants $\mathbf{S}$,$\{\mathbf{A}_\mathrm{i}\}_{i\in\mathcal{A}}$ and $\{\mathbf{P}_\mathrm{i}\}_{i\in\mathcal{P}}$. The meaning of these constants is established by adding the following axioms:

$$\mathbf{S} = 1\text{'}_\mathsf{U} \quad \text{(Ax. 16)}$$

$$Dom(\mathbf{P}_\mathrm{i}) \leq \mathbf{S}, \text{ for all } i \in \mathcal{P} \quad \text{(Ax. 17)}$$

$$\mathbf{1};\mathbf{P}_\mathrm{i} = \mathbf{1}, \text{ for all } i \in \mathcal{P} \quad \text{(Ax. 18)}$$

$$\mathbf{S};\mathbf{A}_\mathrm{i};\mathbf{S} = \mathbf{A}_\mathrm{i}, \text{ for all } i \in \mathcal{A} \quad \text{(Ax. 19)}$$

Axiom (16) establishes that the states are the urelements. Axiom (17) establishes that domains of relations $\mathbf{P}_\mathrm{i}$ are sets of states. Axiom (18) establishes that relations $\mathbf{P}_\mathrm{i}$ are right ideal. Finally, axiom (19) establishes that $\mathbf{A}_\mathrm{i}$ is a binary relation on states.

Definition 3.3 *By ω-CCFA^{+PDL} we denote the extension of ω-CCFA obtained by adding symbols $\mathbf{S}$, $\{\mathbf{A}_\mathrm{i}\}_{i\in\mathcal{A}}$, $\{\mathbf{P}_\mathrm{i}\}_{i\in\mathcal{P}}$ as constants, and adding axioms (or axiom schemes) (16) to (19).*

Definition 3.4 *We define the translation T_{PDL} mapping formulas from PDL(Σ) to relations of ω-CCFA^{+PDL}, as follows:*

- $T_{PDL}(p_i) = \mathbf{P}_\mathrm{i}$
- $T_{PDL}(\neg\alpha) = \mathbf{S};\overline{T_{PDL}(\alpha)}$
- $T_{PDL}(\alpha \vee \beta) = T_{PDL}(\alpha) + T_{PDL}(\beta)$
- $T_{PDL}(\langle r\rangle\alpha) = M_{PDL}(r);T_{PDL}(\alpha)$
- $M_{PDL}(a_i) = \mathbf{A}_\mathrm{i}$
- $M_{PDL}(r \cup s) = M_{PDL}(r) + M_{PDL}(s)$

- $M_{PDL}(r;s) = M_{PDL}(r);M_{PDL}(s)$
- $M_{PDL}(r^*) = (M_{PDL}(r))^*$
- $M_{PDL}(\alpha?) = T_{PDL}(\alpha)\cdot\mathbf{S}$

Lemma 3.1 **([FO98])** *Given a Kripke structure $K = \langle S, \tilde{A}, \tilde{P}\rangle$, there exists a non empty class of proper closure fork algebras extended with constants $\mathbf{S}$, $\{\mathbf{A_i}\}_{i\in\mathcal{A}}$ and $\{\mathbf{P_i}\}_{i\in\mathcal{P}}$ such that, for all $\mathfrak{A}$ in this class,*

- *$\mathfrak{A}$ satisfies Axs. (16)-(19),*
- *for all $q \in S$*
$$K, q \models_{PDL} \alpha \iff q \in \mathsf{dom}\,(T_{PDL}(\alpha))$$

Given a Kripke structure K, we denote the subclass of PCFA determined by Lemma 3.1 by $\mathfrak{C}_K$.

Lemma 3.2 *Given a Kripke structure $K = \langle S, \tilde{A}, \tilde{P}\rangle$, and let $\mathfrak{A} \in \mathfrak{C}_K$, for all $P \in PrgPDL(\Sigma)$,*

$$\langle q, q'\rangle \in Prg_K(P) \iff \langle q, q'\rangle \in M_{PDL}(P)$$

Proof. It follows from definition of $\mathfrak{C}_K$, Prg_K and M_{PDL}. ■

Lemma 3.3 **([FO98])** *Given $\mathfrak{A}$ proper closure fork algebra extended with constants $\mathbf{S}$, $\{\mathbf{A_i}\}_{i\in\mathcal{A}}$ and $\{\mathbf{P_i}\}_{i\in\mathcal{P}}$ satisfying Axs. (16)-(19), there exists a Kripke structure K such that for all $q \in \mathsf{dom}\,(\mathbf{S})$,*

$$q \in \mathsf{dom}\,(T_{PDL}(\alpha)) \iff K, q \models_{PDL} \alpha$$

Theorem 3.1 **([FO98, Thm. 7.15])** *Let $\varphi \in ForPDL(\Sigma)$. Then,*

$$\models_{PDL} \varphi \quad \iff \quad \vdash_{\omega\text{-CCFA}^{+PDL}} \mathbf{S};T_{PDL}(\varphi) = \mathbf{S};\mathbf{1}$$

4 Interpreting LTL in Fork Algebras

The syntax and semantics of linear temporal logic (LTL) were introduced in [Eme90]. LTL is a formalism suitable for reasoning about system behaviors.

Along this section we will assume a fixed (but arbitrary) finite set of atomic proposition symbols $P = \{p_i\}_{i \in \mathcal{P}}$.

Definition 4.1 *The sets of formulas on P is the smallest set $ForLTL(P)$ satisfying:*

- $P \subseteq ForLTL(P)$
- *If* $\{\alpha, \beta\} \subseteq ForLTL(P)$, *then* $\{\neg\alpha, \alpha \vee \beta, \oplus\alpha, \alpha \mathsf{U} \beta\} \subseteq ForLTL(P)$

The semantics of LTL formulas is defined over a Kripke structure K of the form $\langle S, T, S_0, \tilde{P}\rangle$, where S is the set of states, $T \subseteq S \times S$ is the transition relation, $S_0 \subseteq S$ is the set of initial states, $\tilde{P} = \{\tilde{p_i}\}_{i \in \mathcal{P}}$ where $\tilde{p_i} \subseteq S$ for all $i \in \mathcal{P}$. The transition relation T is assumed to be complete; that is, every state has at least one successor.

Given a Kripke structure K and a set P, we can map P to $\tilde{P}$ trivially using the subindexes.

Given a Kripke structure K, the set of traces of K is denoted by Δ_K. A trace $s \in \Delta_K$ is a infinite sequence $s_0, s_1, \ldots$ such that $s_i \in S$ and $\langle s_i, s_{i+1}\rangle \in T$ for all $i \geq 0$. We denote by s^i the suffix of s starting at position i. Similarly, we denote by s_i, the i-th state in the trace s.

Definition 4.2 *Given a Kripke structure K for a set of atomic proposition symbols P and $s \in \Delta_K$, the semantics of a LTL formula is defined recursively as follows:*

- $K, s \models_{LTL} p_i$ *iff* $s_0 \in \tilde{p_i}$
- $K, s \models_{LTL} \neg\alpha$ *iff* $K, s \not\models_{LTL} \neg\alpha$
- $K, s \models_{LTL} \alpha \vee \beta$ *iff* $K, s \models_{LTL} \alpha$ *or* $K, s \models_{LTL} \beta$
- $K, s \models_{LTL} \oplus\alpha$ *iff* $K, s^1 \models_{LTL} \alpha$
- $K, s \models_{LTL} \alpha \mathsf{U} \beta$ *iff there exists* $i \geq 0$ *such that* $K, s^i \models_{LTL} \beta$ *and for all* j *such that* $0 \geq j < i$, $K, s^j \models_{LTL} \alpha$

A formula is satisfied in a Kripke structure K if there exists $s = s_0 s_1 \cdots \in \Delta_K$ such that $s_0 \in S_0$ and $K, s \models_{LTL} \alpha$. A formula is valid in a Kripke structure K if it is satisfied along all traces $s \in \Delta_K$ such that $s_0 \in S_0$. We will use $\Diamond P$ as a shorthand for **true** U P and $\Box P$ for $\neg\Diamond\neg P$.

In [FP03] Frias and Lopez Pombo defined a translation from LTL formulas to fork algebra terms and presented a interpretability theorem for LTL logic into fork algebra. In the same way, in [FP], both authors presented a similar result for the FOLTL logic.

In order to do so, they extended the language of omega closure fork algebras with new constants: $\mathbf{S}$, $\mathbf{T}$, $\mathbf{S_0}$, $\mathbf{tr}$ and a family of constants $\{\mathbf{P_i}\}_{i\in\mathcal{P}}$.

Using Axs. (16)-(18), it can be established that

- the set of states ($\mathbf{S}$) are the urelements,
- the domain of the family of relations $\mathbf{P_i}$ are states, and
- relations $\mathbf{P_i}$ are right-ideal.

In order to give meaning to the remaining constants, the next axioms are introduced:

$$\mathbf{S_0} \leq \mathbf{S} \qquad \text{(Ax. 20)}$$

$$Dom\,(\mathbf{T}) = \mathbf{S}. \qquad \text{(Ax. 21)}$$

Axiom (20) establishes that every initial state is in fact a state and axiom (21) establishes that every state has at least one successor.

The constant relation symbol $\mathbf{tr}$ is added to represent the set of all traces. Given a fork algebra $\mathfrak{A}$, traces can be modeled using infinite right degenerate trees. The leaves in these trees are elements from $U_{\mathfrak{A}}$.

In order to complete the notion of trace in fork algebras, more axioms can be used. In [FP03], a set of axioms was originally presented. In [FP] this set was improved:

$$\mathbf{tr} \leq 1' \qquad \text{(Ax. 22)}$$

$$\breve{\pi}\,;\mathbf{tr}\,;\pi = \mathbf{S} \qquad \text{(Ax. 23)}$$

$$\mathbf{tr} \leq \mathbf{S}\otimes\mathbf{tr} \qquad \text{(Ax. 24)}$$

$$\mathbf{tr}\,;\rho = Ran\,(\pi\,\nabla\,(\mathbf{T}\otimes\rho))\,;\rho\,;\mathbf{tr} \qquad \text{(Ax. 25)}$$

Axiom (22) states that $\mathbf{tr}$ ia a partial identity (a set). Axiom (23) establishes that every element in a trace is a state, and therefore by axiom (16) a urelement. Axiom (24) and (25) establish that traces are infinite, T-related, sequences.

Definition 4.3 *By ω-CCFA^{+LTL} we denote the extension of ω-CCFA obtained by adding symbols $\mathbf{S}$, $\mathbf{T}$, $\mathbf{S_0}$, $\mathbf{tr}$ and a family of constants $P' = \{\mathbf{P_i}\}_{i\in\mathcal{P}}$ as constants, and Axs. (16)-(18) and Axs. (20)-(25).*

Definition 4.4 *We define the translation T_{LTL} mapping formulas from LTL to relations of ω-CCFA^{+LTL}, as follows:*

- $T_{LTL}(p_i) = \pi;\mathbf{P_i}$
- $T_{LTL}(\neg\alpha) = \mathbf{tr};\overline{T_{LTL}(\alpha)}$
- $T_{LTL}(\alpha \vee \beta) = T_{LTL}(\alpha)+T_{LTL}(\beta)$
- $T_{LTL}(\oplus\alpha) = \rho;T_{LTL}(\alpha)$
- $T_{LTL}(\alpha \,\mathsf{U}\, \beta) = (Dom\,(T_{LTL}(\alpha))\,;\rho)^*;T_{LTL}(\beta)$

Definition 4.5 (Infinite trees) *Let S be a nonempty set and T a binary relation on S. Let $\mathcal{T}(S,T)$ be the set of binary trees t satisfying:*

- *t is a binary tree with information in the leaves,*
- *t has infinite height,*
- *leaves are labelled with elements from S,*
- *t is right degenerate,*
- *given two consecutive leaves of t holding information s and s', $\langle s,s'\rangle \in T$*

Definition 4.6 *Let S be a nonempty set, T a binary relation on S and $s = s_0, s_1, s_2, \ldots$ a sequence of T-connected elements of S. We define $t_s \in \mathcal{T}(S,T)$ as the tree satisfying $(\forall i < \omega)(\pi(\rho^i(t_s)) = s_i)$.*

Lemma 4.1 ([FP03, Lemma 6]) *Given a Kripke structure $K = \langle S, T, S_0, \tilde{P}\rangle$, there exists a non empty class of proper closure fork algebra extended with constants $\mathbf{S}$, $\mathbf{T}$, $\mathbf{S_0}$, $\mathbf{tr}$ and $\{\mathbf{P_i}\}_{i\in\mathcal{P}}$ such that, for all $\mathfrak{A}$ in this class,*

- *$\mathfrak{A}$ satisfies Axs. (16)-(18) and Axs. (20)-(25)*
- *for all $s \in \Delta_K$*

$$K, s \models_{LTL} \alpha \iff t_s \in \mathsf{dom}\,(T_{LTL}(\alpha))$$

Given a Kripke structure K, we denote the subclass of PCFA determined by Lemma 4.1 by $\mathfrak{C}_K$.

Definition 4.7 *Let S be a nonempty set. Let T be a binary relation on S. Let $t \in \mathcal{T}(S,T)$. We define s_t as the sequence of states satisfying*

$$(\forall i < \omega)((s_t)_i = \pi(\rho^i(t)))\ .$$

Lemma 4.2 ([FP03, Lemma 5]) *Given $\mathfrak{A} \in$ PCFA extended with constants $\mathbf{S}$, $\mathbf{T}$, $\mathbf{S_0}$, $\mathbf{tr}$ and $\{\mathbf{P_i}\}_{i\in\mathcal{P}}$ satisfying Axs. (16)-(18) and Axs. (20)-(25), there exists a Kripke structure K such that for all $t \in \mathsf{dom}\,(\mathbf{tr})$,*

$$t \in \mathsf{dom}\,(T_{LTL}(\alpha)) \iff K, s_t \models_{LTL} \alpha$$

In order to reduce notation we will denote the relation $Dom(\pi ; \mathbf{S_0}) ; \mathbf{tr}$ as $\mathbf{tr_0}$.

Theorem 4.1 ([FP03, Thm. 3]) *Let $\alpha \in ForLTL(P)$. Then,*

$$\models_{LTL} \alpha \iff \vdash_{\omega\text{-CCFA}+LTL} \mathbf{tr_0} ; T_{LTL}(\alpha) = \mathbf{tr_0} ; \mathbf{1}$$

5 Interpreting DLTL in Fork Algebras

In this section we present the interpretability result for propositional dynamic linear time logic (DLTL) [HT99]. In order to do so, we will define a translation of DLTL formulas to relational expressions.

DLTL is a simple extension the logic of LTL. The main goal of this formalism is to add dynamic behavior to linear temporal time logic. The basic idea is to strengthen the until modality by indexing it with the regular programs of PDL (See def. 3.1).

The syntax of DLTL is defined over a set of atomic propositios $P = \{p_i\}_{i \in \mathcal{P}}$ and a set of atomic actions $A = \{a_i\}_{i \in \mathcal{A}}$. Along this section we will assume a fixed (but arbitrary) finite signature $\Sigma = \langle A, P \rangle$.

Definition 5.1 *The set of programs on* Σ *is the smallest set* $PrgDLTL(\Sigma)$ *satisfying:*

- $A \subseteq PrgDLTL(\Sigma)$
- *If* $r, s \in PrgDLTL(\Sigma)$*, then* $\{r^*, r \cup s, r; s\} \subseteq PrgDLTL(\Sigma)$

Definition 5.2 *The set of formulas on* Σ *is the smallest set* $ForDLTL(\Sigma)$ *satisfying:*

- $P \subseteq ForDLTL(\Sigma)$
- *If* $\alpha, \beta \in ForDLTL(\Sigma)$ *and* $R \in PrgDLTL(\Sigma)$*, then* $\{\neg\alpha, \alpha \vee \beta, \alpha \mathsf{U}^R \beta\} \subseteq ForDLTL(\Sigma)$

The semantics of $DLTL(\Sigma)$ formulas is defined over a Kripke structure K of the form $\langle S, \tilde{A}, S_0, \tilde{P} \rangle$, where

- S is a set of states,
- $\tilde{A} = \{\tilde{a_i}\}_{i \in \mathcal{A}}$ is a set of binary relations on S characterizing atomic actions. It is assumed that every state q has at least one atomic action $\tilde{a} \in \tilde{A}$ such that $q \in \mathsf{dom}\,(\tilde{a})$
- $S_0 \subseteq S$ is the set of initial states and
- $\tilde{P} = \{\tilde{p_i}\}_{i \in \mathcal{P}}$ where $\tilde{p_i} \subseteq S$.

Given a Kripke structure K and a signature Σ, we can map A to $\tilde{A}$ and P to $\tilde{P}$ using the subindexes.

Given a Kripke structure K, the set of traces of K is denoted by Δ_K. A trace $s \in \Delta_K$ is a infinite sequence $s_0, s_1, \ldots$ such that for all $i \geq 0$ $s_i \in S$ and there exists $\tilde{a} \in \tilde{A}$ such that $\langle s_i, s_{i+1} \rangle \in \tilde{a}$. The set of trace prefixes of K is denoted by Γ_K. A trace prefix $\tau \in \Gamma_K$ is a finite sequence such that it is a prefix of a trace in Δ_K. If τ is a trace prefix, then the length of τ is denoted as $|\tau|$.

Definition 5.3 (Trace prefix concatenation) *Let* $\tau, \tau' \in \Gamma_K$

$$\tau;\tau' = \begin{cases} \lambda & \text{if } \tau = \lambda \text{ and } \tau' = \lambda \\ \tau & \text{if } \tau \neq \lambda \text{ and } \tau' = \lambda \\ \tau' & \text{if } \tau = \lambda \text{ and } \tau' \neq \lambda \\ \tau\&(\tau')^1 & \text{if } \tau \neq \lambda \text{ and } \tau' \neq \lambda \text{ and } \tau_{|\tau|-1} = \tau'_0 \\ \bot & \text{otherwise} \end{cases}$$

No confusion should arise from using symbol ; for relational composition and also trace prefix concatenation.

We extend the trace prefix concatenation to sets of trace prefixes.

Definition 5.4 (Trace prefix set concatenation) *Let* $E, E' \subseteq \Gamma_K$.

$$E; E' \quad = \{\tau;\tau' | (\tau \in E \wedge \tau' \in E') \wedge (\tau = \lambda \vee \tau' = \lambda \vee \tau_{|\tau|-1} = \tau'_0)\}$$

Definition 5.5 *We define the i-th folded concatenation of a trace prefix set E (denoted as* $E^{;i}$*) by the conditions:*

$$\begin{aligned} E^{;0} &= \{\lambda\} \\ E^{(;n+1)} &= E; E^{;n} \end{aligned}$$

Definition 5.6 *Given a Kripke structure K for the signature* Σ *and a program* $P \in PrgDLTL(\Sigma)$*, the set of all possible trace prefixes from program P (denoted by* $\|P\|_K$*) is defined recursively as follows:*

- $\|a_i\|_K = \{pq | \langle p, q\rangle \in \tilde{a_i}\}$
- $\|R \cup S\|_K = \|R\|_K \cup \|S\|_K$
- $\|R; S\|_K = \|R\|_K; \|S\|_K$
- $\|R^*\|_K = (\|R\|_K)^* = \bigcup_{i \geq 0}(\|R\|_K)^{;i}$

Definition 5.7 (Trace prefix function) *Let s be a trace in K and* $i \in \mathbb{N}$

$$exec(s, i) = \begin{cases} \lambda & \text{if } i = 0 \\ s_0 \ldots s_i & \text{if } i > 0 \end{cases}$$

Definition 5.8 *Given a Kripke structure K for the signature* Σ *and* $s \in \Delta_K$*, the semantics of a DLTL formula is defined recursively as follows:*

- $K, s \models_{DLTL} p_i$ *iff* $s_0 \in \tilde{p_i}$
- $K, s \models_{DLTL} \neg\alpha$ *iff* $K, s \not\models_{DLTL} \alpha$
- $K, s \models_{DLTL} \alpha \vee \beta$ *iff* $K, s \models_{DLTL} \alpha$ *or* $K, s \models_{DLTL} \beta$
- $K, s \models_{DLTL} \alpha \, \mathsf{U}^P \, \beta$ *iff exists* $i \geq 0$ *such that*

- $K, s^i \models_{DLTL} \beta$
- *for all j such that* $0 \leq j < i$ *then* $K, s^j \models_{DLTL} \alpha$
- $exec(s, i) \in \|P\|_K$

As in LTL, a formula is satisfied in a Kripke structure K if there exists $s = s_0 s_1 \cdots \in \Delta_K$ such that $s_0 \in S_0$ and $K, s \models_{DLTL} \alpha$. A formula is valid in a Kripke structure K if it is satisfied along all traces $s \in \Delta_K$ such that $s_0 \in S_0$.

In [HT99] the interpretability of LTL in DLTL is presented.

Definition 5.9 *We define the translation* $T_{LTL \to DLTL}$ *mapping formulas from* LTL *to formulas in* $DLTL$*, as follows:*

- $T_{LTL \to DLTL}(p_i) = p_i$
- $T_{LTL \to DLTL}(\neg\alpha) = \neg T_{LTL \to DLTL}(\alpha)$
- $T_{LTL \to DLTL}(\alpha \vee \beta) = T_{LTL \to DLTL}(\alpha) \vee T_{LTL \to DLTL}(\beta)$
- $T_{LTL \to DLTL}(\oplus\alpha) = \mathbf{true}\ \mathsf{U}^R\ T_{LTL \to DLTL}(\alpha)$*, where* $R = \bigcup_{i \in \mathcal{A}} a_i$
- $T_{LTL \to DLTL}(\alpha\ \mathsf{U}\ \beta) = T_{LTL \to DLTL}(\alpha)\ \mathsf{U}^{R^*}\ T_{LTL \to DLTL}(\beta)$*, where* $R = \bigcup_{i \in \mathcal{A}} a_i$

Theorem 5.1 ([HT99, page 190]) *Given a Kripke structure* K *for* $DLTL(\Sigma)$*. Let* $\alpha \in LTL(P)$*, and let* $s \in \Delta_K$*, then,*

$$K^{LTL}, s \models_{LTL} \alpha \iff K, s \models_{DLTL} T_{LTL \to DLTL}(\alpha)$$

We will interpret $DLTL$ with an extension of ω-CCFA.

Definition 5.10 *By* ω-CCFA^{+DLTL} *we denote the extension of* ω-CCFA *obtained by adding symbols* $\mathbf{S}$, $\mathbf{S_0}$, $\mathbf{tr}$, $\{\mathbf{A_i}\}_{i \in \mathcal{A}}$, $\{\mathbf{P_i}\}_{i \in \mathcal{P}}$ *as constants. The axioms of this theory are the axioms of* ω-CCFA *and:*

- *the axioms of* ω-CCFA^{+PDL}
- *the axioms of* ω-CCFA^{+LTL}
- *the equation*

$$\mathbf{T} = \sum_{i \in \mathcal{A}} \mathbf{A_i}^1 \qquad \textit{(Ax. 26)}$$

Axiom (26) says that two states p and q can be consecutive if there is at least one action in which we can evolve from p to q.

Lemma 5.1 *If* α *is an* ω-CCFA *formula, then*

$$\not\vdash_{\omega\text{-CCFA}^{+DLTL}} \alpha \Longrightarrow \not\vdash_{\omega\text{-CCFA}} \alpha$$

[1] Note that this is an equation because $\mathcal{A}$ is a finite set.

Proof. It follows from ω-CCFA^{+DLTL} being an extension of ω-CCFA. ■

Definition 5.11 *We define the translation T_{DLTL} mapping formulas from $DLTL$ to relations of ω-CCFA^{+DLTL}, as follows:*

- $T_{DLTL}(p_i) = \pi ; \mathbf{P_i}$
- $T_{DLTL}(\neg\alpha) = \mathbf{tr} ; \overline{T_{DLTL}(\alpha)}$
- $T_{DLTL}(\alpha \wedge \beta) = T_{DLTL}(\alpha) + T_{DLTL}(\beta)$
- $T_{DLTL}(\alpha \; \mathsf{U}^P \; \beta) = M_{DLTL}(\alpha, P) ; T_{DLTL}(\beta)$
- $M_{DLTL}(\alpha, a_i) = Dom\,(T_{DLTL}(\alpha))\,;Ran\,(\pi \nabla (\mathbf{A_i} \otimes \rho))\,;\rho$
- $M_{DLTL}(\alpha, R^*) = M_{DLTL}(\alpha, R)^*$
- $M_{DLTL}(\alpha, R \cup S) = M_{DLTL}(\alpha, R) + M_{DLTL}(\alpha, S)$
- $M_{DLTL}(\alpha, R; S) = M_{DLTL}(\alpha, R) ; M_{DLTL}(\alpha, S)$

Lemma 5.2 *Given a Kripke structure $K = \langle S, \tilde{A}, S_0, \tilde{P}\rangle$, there exists a non empty class of proper closure fork algebras extended with constants $\mathbf{S}$, $\mathbf{T}$, $\mathbf{S_0}$, $\mathbf{tr}$, $\{\mathbf{A_i}\}_{i \in \mathcal{A}}$ and $\{\mathbf{P_i}\}_{i \in \mathcal{P}}$, such that, for all $\mathfrak{A}$ in this class,*

- *$\mathfrak{A}$ satisfies Axs. (16)-(26)*
- *for all $s \in \Delta_K$,*

$$K, s \models_{DLTL} \alpha \iff t_s \in \mathsf{dom}\,(T_{DLTL}(\alpha))\,.$$

Proof. See lemma B.11 for a complete proof. ■

Given a Kripke structure K, we denote the subclass of PCFA determined by Lemma 5.2 by $\mathfrak{C}_K$.

Lemma 5.3 *Given $\mathfrak{A} \in$ PCFA extended with constants $\mathbf{S}$, $\mathbf{T}$, $\mathbf{S_0}$, $\mathbf{tr}$, $\{\mathbf{A_i}\}_{i \in \mathcal{A}}$ and $\{\mathbf{P_i}\}_{i \in \mathcal{P}}$ satisfying Axs. (16)-(26), there exists a Kripke structure K such that for all $t \in \mathsf{dom}\,(\mathbf{tr})$,*

$$t \in \mathsf{dom}\,(T_{DLTL}(\alpha)) \iff K, s_t \models_{DLTL} \alpha\ .$$

Proof. See lemma B.10 for a complete proof. ■

Next we present the interpretability theorem for DLTL. It shows that it is possible to replace reasoning both at the logical and metalogical level in DLTL by equational reasoning in our extension of ω-CCFA.

Theorem 5.2 *Let $\alpha \in ForDLTL(\Sigma)$. Then,*

$$\models_{DLTL} \alpha \iff \vdash_{\omega\text{-CCFA}^{+DLTL}} \mathbf{tr_0} ; T_{DLTL}(\alpha) = \mathbf{tr_0} ; \mathbf{1}$$

Proof.

$\Rightarrow$)

First, we assume that

$$\not\vdash_{\omega\text{-CCFA}^{+DLTL}} \mathit{Dom}\left(\pi ; \mathbf{S_0}\right) ; \mathbf{tr} ; T_{DLTL}\left(\alpha\right) = \mathit{Dom}\left(\pi ; \mathbf{S_0}\right) ; \mathbf{tr} ; \mathbf{1}$$

By Lemma 5.1,

$$\not\vdash_{\omega\text{-CCFA}} \mathit{Dom}\left(\pi ; \mathbf{S_0}\right) ; \mathbf{tr} ; T_{DLTL}\left(\alpha\right) = \mathit{Dom}\left(\pi ; \mathbf{S_0}\right) ; \mathbf{tr} ; \mathbf{1}$$

Then, by Thm. 2.9, there exists ω-CCFA model $\langle \mathfrak{A}, m \rangle$ such that

$$\langle \mathfrak{A}, m \rangle \not\models_{\omega\text{-CCFA}} \mathit{Dom}\left(\pi ; \mathbf{S_0}\right) ; \mathbf{tr} ; T_{DLTL}\left(\alpha\right) = \mathit{Dom}\left(\pi ; \mathbf{S_0}\right) ; \mathbf{tr} ; \mathbf{1}$$

By Thm. 2.8 there exists $\mathfrak{B} \in$ PCFA such that $\mathfrak{B}$ is isomorphic to $\mathfrak{A}$, and m' the meaning function isomorphic to m. Hence,

$$\langle \mathfrak{B}, m' \rangle \not\models_{\omega\text{-CCFA}} \mathit{Dom}\left(\pi ; \mathbf{S_0}\right) ; \mathbf{tr} ; T_{DLTL}\left(\alpha\right) = \mathit{Dom}\left(\pi ; \mathbf{S_0}\right) ; \mathbf{tr} ; \mathbf{1}$$

This implies the existence of $t \in U_{\mathfrak{B}}$ satisfying:

- $t \in \mathsf{dom}\left(\mathbf{tr}\right)$
- $\pi(t) \in \mathsf{dom}\left(\mathbf{S_0}\right)$
- $t \notin \mathsf{dom}\left(T_{DLTL}\left(\alpha\right)\right)$

By Lemma 5.3 there exists a Kripke structure K such that

$$K, s_t \not\models_{DLTL} \alpha$$

Thus, since $(s_t)_0 \in S_0$

$$\not\models_{DLTL} \alpha$$

$\Leftarrow$)

We begin by assuming that

$$\not\models_{DLTL} \alpha$$

Then, there exists a Kripke structure $K = \langle S, T, S_0, \tilde{A} \rangle$ and a trace $s \in \Delta_K$ with $s_0 \in S_0$ such that

$$K, s \not\models_{DLTL} \alpha$$

By Lemma 5.2, there exists $\mathfrak{A} \in$ PCFA extended with constants $\mathbf{S}$, $\mathbf{T}$, $\mathbf{S_0}$, $\mathbf{tr}$, $\{\mathbf{A_i}\}_{i \in \mathcal{A}}$ and $\{\mathbf{P_i}\}_{i \in \mathcal{P}}$ satisfying the axioms of ω-CCFA^{+DLTL}, such that

$$t_s \notin \mathsf{dom}\left(T_{DLTL}\left(\alpha\right)\right)$$

Since $t_s \in \mathsf{dom}\,(\mathbf{tr})$ and $\pi(t_s) \in \mathsf{dom}\,(\mathbf{S_0})$,

$$\mathfrak{A} \not\models_{\omega\text{-}\mathsf{CCFA}} \mathit{Dom}\,(\pi\,;\mathbf{S_0})\,;\mathbf{tr};T_{DLTL}\,(\alpha) = \mathit{Dom}\,(\pi\,;\mathbf{S_0})\,;\mathbf{tr}\,;\mathbf{1}$$

Hence,

$$\not\models_{\omega\text{-}\mathsf{CCFA}} \mathit{Dom}\,(\pi\,;\mathbf{S_0})\,;\mathbf{tr};T_{DLTL}\,(\alpha) = \mathit{Dom}\,(\pi\,;\mathbf{S_0})\,;\mathbf{tr}\,;\mathbf{1}$$

and Thm. 2.9,

$$\not\vdash_{\omega\text{-}\mathsf{CCFA}} \mathit{Dom}\,(\pi\,;\mathbf{S_0})\,;\mathbf{tr};T_{LTL}(\alpha) = \mathit{Dom}\,(\pi\,;\mathbf{S_0})\,;\mathbf{tr}\,;\mathbf{1}$$

Due to ω-CCFA^{+DLTL} is an extension of ω-CCFA,

$$\not\vdash_{\omega\text{-}\mathsf{CCFA}^{+DLTL}} \mathit{Dom}\,(\pi\,;\mathbf{S_0})\,;\mathbf{tr};T_{LTL}(\alpha) = \mathit{Dom}\,(\pi\,;\mathbf{S_0})\,;\mathbf{tr}\,;\mathbf{1}$$

■

6 Reasoning across dynamic and linear time temporal logics

In this section we reason across PDL and LTL using the language of the *omega closure fork algebras* as an amalgamating formalism. In order to do so, in subsection 6.1 we describe an abstract system and formalize it by means of a PDL theory and a LTL theory. Also, we introduce a desirable system property written in $DLTL$. In subsection 6.2 and 6.3 we verify this property using ω-CCFA^{+DLTL} (ω-CCFA^{+} for short).

6.1 An Abstract System and its Specification

Let $\mathcal{S}$ be a system, such that:

1. There is a set of atomic actions.
2. System state is described by means of a finite set of atomic propositions.
3. Every atomic action has a known precondition and postcondition, both expressed in terms of propositional formulas.
4. We have a linear temporal property I which is invariant under atomic actions, i.e; every time a precondition and I hold in a state, the next state verifies that if the postcondition is reached, then I holds.
5. If the precondition is not met, the atomic action is not enabled and cannot be launched.

Also, it is highly desirable that the next property holds:

"If I holds, then it is invariant over every program."

Now we will present two theories that grasp this system description. In order to do so, and for the rest of this work, we will consider:

- A signature $\Sigma = \langle A, P\rangle$ where $A = \{a_i\}_{i\in\mathcal{A}}$ and $P = \{p_i\}_{i\in\mathcal{P}}$ are sets of symbols, representing atomic actions and atomic propositions mentioned in system description.
- Let $i \in \mathcal{A}$, we have $\alpha_i \in ForProp(P)$ and $\beta_i \in ForProp(P)$ representing precondition and postcondition of action symbol a_i.
- $I \in ForLTL(\Sigma)$ representing the desirable property mentioned in system description.

Definition 6.1 (specPDL Theory) *specPDL is a PDL(Σ) theory, containing the following axioms*

$$\alpha_i \Longrightarrow [a_i]\beta_i, \textit{ for all } i \in \mathcal{A},$$
$$\neg\alpha_i \Longrightarrow [a_i]\textbf{false}, \textit{ for all } i \in \mathcal{A}.$$

Definition 6.2 (specLTL Theory) *specLTL is a LTL(P) theory, containing the following axioms*

$$\Box((\alpha_i \wedge I) \Longrightarrow \oplus(\beta_i \Longrightarrow I)), \text{ for all } i \in \mathcal{A}.$$

Once system features are formalized, it remains to specify the system property we would like to verify, (i.e. if property I holds, it is invariant over every program).

Notice that test programs are not included as DLTL programs. One way to overcome this language constraint is to restrict the proof to a finite set of test programs, and model them as atomic actions.

Definition 6.3 (Test free program) *The set of PDL test free programs for the signature* Σ *is the smallest set* $TestFreePrgPDL(\Sigma)$ *such that:*

- $A \subseteq TestFreePrgPDL(\Sigma)$
- *If* $\{R, S\} \subseteq TestFreePrgPDL(\Sigma)$, *then* $\{R; S, R \cup S, R^*\} \subseteq TestFreePrgPDL(\Sigma)$

We rephrase our goal property as:

If I holds, then I is invariant over every PDL test free program.

Let $I' = T_{LTL \to DLTL}(I)$, and let us consider only PDL test free programs. Then, by Lemma C.3, the desirable system property is stated by means of a DLTL theory as follows:

Definition 6.4 (specDLTL Theory) *specDLTL is a DLTL(Σ) theory, containing the following axioms*

$$(\mathbf{true} \ \mathsf{U}^R \ \mathbf{true}) \Longrightarrow (I' \Longrightarrow I' \ \mathsf{U}^R \ I')$$

for all $R \in PrgDLTL(\Sigma)$.

6.2 Verification of properties through fork reasoning

We begin this subsection by introducing mappings from $DLTL$ models to PDL and LTL models respectively.

Definition 6.5 *Given a Kripke structure* $K = \langle S, \tilde{A}, S_0, \tilde{P} \rangle$ *that is a model for theory* $DLTL(\Sigma)$, *we define* K^{LTL} *as the Kripke structure satisfying*

$$K^{LTL} = \langle S, \bigcup_{i \in \mathcal{A}} \tilde{a_i}, S_0, \tilde{P} \rangle$$

Notice that K^{LTL} is a model for theory $LTL(P)$.

Definition 6.6 *Given a Kripke structure* $K = \langle S, \tilde{A}, S_0, \tilde{P} \rangle$ *that is a model for theory* $DLTL(\Sigma)$, *we define* K^{PDL} *as the Kripke structure satisfying*

$$K^{PDL} = \langle S, \tilde{A}, \tilde{P} \rangle$$

Notice that K^{PDL} is a model for theory $PDL(\Sigma)$.

Once we have defined both system features and its desirable properties, we will prove that in every system that meets system features holds the desirable property. Using model jergon, we need to show that every model of the system features is a model of the desirable property. This notion is formalized by Thm. 6.1.

As shown in appendix E, this proof can be undertaken in a semantic manner. Nevertheless, it is our main intention to show how fork calculus can be useful to replace semantic proving when reasoning across dynamic and linear temporal logics.

The proof of Thm. 6.1 is organized as follows. First, we use the translation of PDL and LTL into fork algebras to homogenize system features (since system features are formalized using only these logics). Secondly, we use the translation of DLTL into fork algebras to see how the desirable property looks like in this relational language. Finally, we use the fork calculus to prove that the relational translation of the property can be deduced from the relational translation of system features (this notion is captured by Thm. 6.2).

Theorem 6.1 *Let K be a Kripke structure that is a model for the theory $DLTL(\Sigma)$, such that*

- *K^{PDL} is a model of specPDL.*
- *K^{LTL} is a model of specLTL.*

Then, K is a model of specDLTL.

Proof. Let $\mathfrak{A} \in \mathfrak{C}_K$. By Lemma C.5, $\mathfrak{A} \in \mathfrak{C}_{K^{PDL}}$. Since K^{PDL} is a model of $specPDL$, then

$$\mathfrak{A} \models_{\omega\text{-CCFA+}} \mathbf{S}\,;T_{PDL}(\alpha_i \Longrightarrow [a_i]\beta_i) = \mathbf{S}\,;\mathbf{1}$$

and,

$$\mathfrak{A} \models_{\omega\text{-CCFA+}} \mathbf{S}\,;T_{PDL}(\neg\alpha_i \Longrightarrow [a_i]\mathbf{false}) = \mathbf{S}\,;\mathbf{1}$$

By Lemma C.4, $\mathfrak{A} \in \mathfrak{C}_{K^{LTL}}$. Since K^{LTL} is a model of $specLTL$, then

$$\mathfrak{A} \models_{\omega\text{-CCFA+}} \mathbf{tr_0}\,;T_{LTL}(\Box(\alpha_i \wedge I \Longrightarrow \oplus(\beta_i \Longrightarrow I))) = \mathbf{tr_0}\,;\mathbf{1}$$

By Thm. C.1,

$$\vdash_{\omega\text{-CCFA+}} \mathbf{S}\,;T_{PDL}(\alpha_i \Longrightarrow [a_i]\beta_i) = \mathbf{S}\,;\mathbf{1}$$
$$\vdash_{\omega\text{-CCFA+}} \mathbf{S}\,;T_{PDL}(\neg\alpha_i \Longrightarrow [a_i]\mathbf{false}) = \mathbf{S}\,;\mathbf{1}$$
$$\vdash_{\omega\text{-CCFA+}} \mathbf{tr_0}\,;T_{LTL}(\Box(\alpha_i \wedge I \Longrightarrow \oplus(\beta_i \Longrightarrow I))) = \mathbf{tr_0}\,;\mathbf{1}$$

Thus, by Thm. 6.2,

$$\vdash_{\omega\text{-CCFA+}} \mathbf{tr_0}\,;T_{DLTL}\left((\mathbf{true}\ \mathsf{U}^R\ \mathbf{true}) \Longrightarrow (I' \Longrightarrow I'\ \mathsf{U}^R\ I')\right) = \mathbf{tr_0}\,;\mathbf{1}$$

By ω-CCFA$^+$ completeness (Thm. C.1)

$$\mathfrak{A} \models_{\omega\text{-CCFA}^+} \mathbf{tr_0};T_{DLTL}\left((\mathbf{true}\ \mathsf{U}^R\ \mathbf{true}) \Longrightarrow (I' \Longrightarrow I'\ \mathsf{U}^R\ I')\right) = \mathbf{tr_0};\mathbf{1}$$

Then, by Lemma 5.3, there exists a Kripke structure $K' = \langle S', \tilde{A}', S'_0, \tilde{P}' \rangle$ such that, for all $s \in \Delta_{K'}$, for all $R \in PrgDLTL(\Sigma)$,

$$K', s \models_{DLTL} (\mathbf{true}\ \mathsf{U}^R\ \mathbf{true}) \Longrightarrow (I' \Longrightarrow I'\ \mathsf{U}^R\ I')$$

We finish this proof by showing that if a formula is valid in K', it is also valid in K.

Let α a $DLTL$ formula, $s \in \Delta_{K'}$,

$$\begin{aligned} & K', s \models_{DLTL} \alpha \\ \Longleftrightarrow & t_s \in \mathsf{dom}\left(T_{DLTL}\left(\alpha\right)\right) && \text{(by Lemma 5.3)} \\ \Longleftrightarrow & K, s \models_{DLTL} \alpha && \text{(by def. } \mathfrak{C}_{DLTL}\text{)} \end{aligned}$$

Therefore, K is a model of $specDLTL$. ■

6.3 Reasoning across formalisms: Fork assault

We dedicate this subsection to present and prove Thm. 6.2. This theorem captures how the relational translation of the property can be deduced from the relational translation of system features using fork calculus only, and it is essential to a fork algebraic proof of Thm. 6.1.

We begin by introducing some intermediate lemmas.

Lemma 6.1 *Let $i \in \mathcal{A}$. Then,*

$$\begin{aligned} & \mathbf{S};T_{PDL}(\alpha_i \Longrightarrow [a_i]\beta_i) = \mathbf{S};\mathbf{1}, \\ & \mathbf{S};T_{PDL}(\neg\alpha_i \Longrightarrow [a_i]\mathbf{false}) = \mathbf{S};\mathbf{1} \\ \vdash_{\omega\text{-CCFA}^+} & \\ & \mathbf{A_i} = Dom\left(T_{PDL}(\alpha_i)\right);\mathbf{A_i};Dom\left(T_{PDL}(\beta_i)\right) \end{aligned}$$

Proof. We proceed as follows.

$$\begin{aligned} & \mathbf{S};T_{PDL}(\alpha_i \Longrightarrow [a_i]\beta_i) \\ = & \mathbf{S};T_{PDL}(\neg\alpha_i \vee \neg\langle a_i\rangle\neg\beta_i) \\ = & \mathbf{S};(T_{PDL}(\neg\alpha_i) + T_{PDL}(\neg\langle a_i\rangle\neg\beta_i)) && \text{(by def. } T_{PDL}\text{)} \\ = & \mathbf{S};\mathbf{S};\overline{T_{PDL}(\alpha_i)} + \mathbf{S};\overline{T_{PDL}(\langle a_i\rangle\neg\beta_i)} && \text{(by def. } T_{PDL}\text{)} \\ = & \mathbf{S};\overline{T_{PDL}(\alpha_i)} + \mathbf{S};\overline{M_{PDL}(a_i);T_{PDL}(\neg\beta_i)} && \text{(by Thm. A.2.7 and def. } T_{PDL}\text{)} \\ = & \mathbf{S};\overline{T_{PDL}(\alpha_i)} + \mathbf{S};\overline{\mathbf{A_i};\mathbf{S};\overline{T_{PDL}(\beta_i)}} && \text{(by def. } T_{PDL} \text{ and } M_{PDL}\text{)} \end{aligned}$$

Hence,

$$\mathbf{S};\overline{T_{PDL}(\alpha_i)}+\mathbf{S};\overline{\mathbf{A_i};\mathbf{S};\overline{T_{PDL}(\beta_i)}} = \mathbf{S};\mathbf{1} \tag{1}$$

We also have

$$\begin{aligned}
\mathbf{S} &= \mathit{Dom}\,(\mathbf{S}) && \text{(by Lemma A.1.1)}\\
&= \mathit{Dom}\,(\mathbf{S};\mathbf{1}) && \text{(by Lemma A.1.14)}\\
&= \mathit{Dom}\,(\mathbf{S};T_{PDL}(\neg\alpha_i \implies [a_i]\mathbf{false})) && \text{(by Hyp.)}\\
&= \mathit{Dom}\,(\mathbf{S};T_{PDL}(\alpha_i \vee \neg\langle a_i\rangle\mathbf{true})) && \\
&= \mathit{Dom}\left(\mathbf{S};(T_{PDL}(\alpha_i)+\mathbf{S};\overline{\mathbf{A_i};\mathbf{S};\mathbf{1}})\right) && \text{(by def. } T_{PDL})\\
&= \mathbf{S};\mathit{Dom}\left(T_{PDL}(\alpha_i)+\mathbf{S};\overline{\mathbf{A_i};\mathbf{S};\mathbf{1}}\right) && \text{(by Lemma A.1.4)}\\
&= \mathbf{S};(\mathit{Dom}\,(T_{PDL}(\alpha_i)) + \mathit{Dom}\left(\mathbf{S};\overline{\mathbf{A_i};\mathbf{S};\mathbf{1}}\right)) && \text{(by Thm. A.1.12)}\\
&= \mathbf{S};(\mathit{Dom}\,(T_{PDL}(\alpha_i)) + \mathbf{S};\mathit{Dom}\left(\overline{\mathbf{A_i};\mathbf{S};\mathbf{1}}\right)) && \text{(by Lemma A.1.4)}\\
&= \mathbf{S};\mathit{Dom}\,(T_{PDL}(\alpha_i)) + \mathbf{S};\mathbf{S};\mathit{Dom}\left(\overline{\mathbf{A_i};\mathbf{S};\mathbf{1}}\right) && \text{(by Lemma A.1.13)}\\
&= \mathbf{S};\mathit{Dom}\,(T_{PDL}(\alpha_i)) + \mathbf{S};\mathit{Dom}\left(\overline{\mathbf{A_i};\mathbf{S};\mathbf{1}}\right) && \text{(by Thm. A.2.7)}\\
&= \mathbf{S};\mathit{Dom}\,(T_{PDL}(\alpha_i)) + \mathbf{S};\neg\mathit{Dom}\,(\mathbf{A_i};\mathbf{S};\mathbf{1}) && \text{(by Thm. A.3.2)}\\
&= \mathbf{S};\mathit{Dom}\,(T_{PDL}(\alpha_i)) + \mathbf{S};\neg\mathit{Dom}\,(\mathbf{A_i};\mathbf{S}) && \text{(by Lemma A.1.14)}\\
&= \mathbf{S};\mathit{Dom}\,(T_{PDL}(\alpha_i)) + \mathbf{S};\neg\mathit{Dom}\,(\mathbf{A_i}) && \text{(by Lemma D.13)}
\end{aligned}$$

Thus,

$$\mathbf{S} = \mathbf{S};\mathit{Dom}\,(T_{PDL}(\alpha_i)) + \mathbf{S};\neg\mathit{Dom}\,(\mathbf{A_i}) \tag{2}$$

Then,

$$\begin{aligned}
\mathit{Dom}\,(\mathbf{A_i}) &= \mathit{Dom}\,(\mathbf{A_i})\,;\mathbf{S} && \text{(by Lemma D.14)}\\
&= \mathit{Dom}\,(\mathbf{A_i})\,;(\mathbf{S};\mathit{Dom}\,(T_{PDL}(\alpha_i)) + \mathbf{S};\neg\mathit{Dom}\,(\mathbf{A_i})) && \text{(by (2))}\\
&= \mathit{Dom}\,(\mathbf{A_i})\,;\mathbf{S};\mathit{Dom}\,(T_{PDL}(\alpha_i)) + \mathit{Dom}\,(\mathbf{A_i})\,;\mathbf{S};\neg\mathit{Dom}\,(\mathbf{A_i}) && \\
& && \text{(by Lemma A.1.13)}\\
&= \mathit{Dom}\,(\mathbf{A_i})\,;\mathit{Dom}\,(T_{PDL}(\alpha_i)) + \mathit{Dom}\,(\mathbf{A_i})\,;\neg\mathit{Dom}\,(\mathbf{A_i}) && \\
& && \text{(by Lemma D.14)}\\
&= \mathit{Dom}\,(\mathbf{A_i})\,;\mathit{Dom}\,(T_{PDL}(\alpha_i)) + \mathit{Dom}\,(\mathbf{A_i})\cdot\neg\mathit{Dom}\,(\mathbf{A_i}) && \\
& && \text{(by Thm. A.1.7)}\\
&= \mathit{Dom}\,(\mathbf{A_i})\,;\mathit{Dom}\,(T_{PDL}(\alpha_i)) && \text{(by Thm. A.2.2)}
\end{aligned}$$

Therefore,

$$\mathit{Dom}\,(\mathbf{A_i}) = \mathit{Dom}\,(\mathbf{A_i})\,;\mathit{Dom}\,(T_{PDL}(\alpha_i)) \tag{3}$$

In order to prove the lemma we will prove both inclusions.

$\geq$)

$$\mathit{Dom}\,(T_{PDL}(\alpha_i))\,;\mathbf{A_i};\mathit{Dom}\,(T_{PDL}(\beta_i)) \leq \mathbf{A_i} \qquad \text{(by Thm. A.2.8)}$$

$\leq$)

$$
\begin{aligned}
\mathbf{A_i} &= Dom(\mathbf{A_i})\,;\mathbf{A_i} && \text{(by Thm. A.1.11)}\\
&= Dom(\mathbf{A_i})\,;Dom(T_{PDL}(\alpha_i))\,;\mathbf{A_i} && \text{(by (3))}\\
&= Dom(T_{PDL}(\alpha_i))\,;\mathbf{A_i} && \text{(by Lemma A.2.5 and Thm. A.1.11)}\\
&= Dom(T_{PDL}(\alpha_i))\,;\mathbf{S};\mathbf{A_i} && \text{(by Lemma D.12)}\\
&= Dom(T_{PDL}(\alpha_i))\,;Dom(\mathbf{S})\,;\mathbf{A_i} && \text{(by Lemma A.1.1)}\\
&= Dom(T_{PDL}(\alpha_i))\,;Dom(\mathbf{S};\mathbf{1})\,;\mathbf{A_i} && \text{(by Lemma. A.1.14)}\\
&= Dom(T_{PDL}(\alpha_i))\,;Dom\left(\mathbf{S};\overline{T_{PDL}(\alpha_i)}+\mathbf{S};\overline{\mathbf{A_i};\mathbf{S};\overline{T_{PDL}(\beta_i)}}\right);\mathbf{A_i} && \text{(by (1))}\\
&= Dom(T_{PDL}(\alpha_i))\,;\left(\begin{array}{l} Dom\left(\mathbf{S};\overline{T_{PDL}(\alpha_i)}\right)\\ +Dom\left(\mathbf{S};\overline{\mathbf{A_i};\mathbf{S};\overline{T_{PDL}(\beta_i)}}\right)\end{array}\right);\mathbf{A_i} && \text{(by Thm. A.1.12)}\\
&= Dom(T_{PDL}(\alpha_i))\,;Dom\left(\mathbf{S};\overline{T_{PDL}(\alpha_i)}\right);\mathbf{A_i}\\
&\qquad +Dom(T_{PDL}(\alpha_i))\,;Dom\left(\mathbf{S};\overline{\mathbf{A_i};\mathbf{S};\overline{T_{PDL}(\beta_i)}}\right);\mathbf{A_i} && \text{(by Lemma A.1.13)}\\
&= Dom(T_{PDL}(\alpha_i))\,;\mathbf{S};Dom\left(\overline{T_{PDL}(\alpha_i)}\right);\mathbf{A_i}\\
&\qquad +Dom(T_{PDL}(\alpha_i))\,;\mathbf{S};Dom\left(\overline{\mathbf{A_i};\mathbf{S};\overline{T_{PDL}(\beta_i)}}\right);\mathbf{A_i} && \text{(by Lemma A.1.4)}\\
&= \mathbf{S};(Dom(T_{PDL}(\alpha_i))\cdot\neg Dom(T_{PDL}(\alpha_i)));\mathbf{A_i}\\
&\qquad +Dom(T_{PDL}(\alpha_i))\,;\mathbf{S};Dom\left(\overline{\mathbf{A_i};\mathbf{S};\overline{T_{PDL}(\beta_i)}}\right);\mathbf{A_i} && \text{(by Thms. A.3.2, A.2.5 and A.1.7)}\\
&= Dom(T_{PDL}(\alpha_i))\,;\mathbf{S};Dom\left(\overline{\mathbf{A_i};\mathbf{S};\overline{T_{PDL}(\beta_i)}}\right);\mathbf{A_i} && \text{(by Thm. A.2.2 and A.1.1)}\\
&= Dom(T_{PDL}(\alpha_i))\,;\mathbf{S};Dom\left(\overline{\mathbf{A_i};\mathbf{S};\overline{T_{PDL}(\beta_i)}}\right);\mathbf{A_i};\mathbf{S} && \text{(by Lemma D.13)}\\
&\leq Dom(T_{PDL}(\alpha_i))\,;\mathbf{S};\mathbf{A_i};\mathbf{S};Dom(T_{PDL}(\beta_i)) && \text{(by Lemma A.1.12)}\\
&= Dom(T_{PDL}(\alpha_i))\,;\mathbf{A_i};Dom(T_{PDL}(\beta_i)) && \text{(by Ax. 19)}
\end{aligned}
$$

■

For the rest of this work, we will reduce notation by using $\mathbf{tr}_{\mathbf{0}}^{\rightarrow}$ to denote relation $Ran(\mathbf{tr_0};\rho^*)$.

Lemma 6.2 *Let $i \in \mathcal{A}$. Then,*

$$\mathbf{tr_0}\,;T_{LTL}(\Box(\alpha_i \wedge I \Longrightarrow \oplus(\beta_i \Longrightarrow I))) = \mathbf{tr_0}\,;\mathbf{1}$$

$$\vdash_{\omega\text{-CCFA+}}$$

$$\overrightarrow{\mathbf{tr_0}} \leq \left(\begin{array}{l} \neg \mathit{Dom}\,(T_{LTL}(\alpha_i)) \\ + \neg \mathit{Dom}\,(T_{LTL}(I)) \\ + \mathit{Dom}\left(\rho;\mathbf{tr};\overline{T_{LTL}(\beta_i)}\right) \\ + \mathit{Dom}\,(\rho;T_{LTL}(I)) \end{array} \right)$$

Proof. In order to prove this property we will show that

$$\mathbf{tr_0}\,;\rho^* \leq \mathbf{tr_0}\,;\rho^*\,; \left(\begin{array}{l} \neg \mathit{Dom}\,(T_{LTL}(\alpha_i)) \\ + \neg \mathit{Dom}\,(T_{LTL}(I)) \\ + \mathit{Dom}\left(\rho;\mathbf{tr};\overline{T_{LTL}(\beta_i)}\right) \\ + \mathit{Dom}\,(\rho;T_{LTL}(I)) \end{array} \right) \qquad (4)$$

We proceed as follows.

$$\begin{array}{ll}
\mathbf{tr_0}\,;\rho^* & \\
= \mathit{Dom}\,(\mathbf{tr_0})\,;\rho^* & \text{(by Lemma A.1.1)} \\
= \mathit{Dom}\,(\mathbf{tr_0};\mathbf{1})\,;\rho^* & \text{(by Lemma A.1.14)} \\
= \mathit{Dom}\,(\mathbf{tr_0};T_{LTL}(\Box(\alpha_i \wedge I \Longrightarrow \oplus(\beta_i \Longrightarrow I))))\,;\rho^* & \text{(by Hyp.)} \\
= \mathit{Dom}\,(\mathbf{tr_0};T_{LTL}(\neg(\mathbf{true}\ \mathsf{U}\ \neg(\neg\alpha_i \vee \neg I \vee \oplus(\neg\beta_i \vee I)))))\,;\rho^* & \text{(by def. } \Longrightarrow \text{ and } \Box\text{)} \\
= \mathbf{tr_0}\,;\mathit{Dom}\,(T_{LTL}(\neg(\mathbf{true}\ \mathsf{U}\ \neg(\neg\alpha_i \vee \neg I \vee \oplus(\neg\beta_i \vee I)))))\,;\rho^* & \text{(by Lemma A.1.4)} \\
= \mathbf{tr_0}\,;\mathit{Dom}\left(\mathbf{tr};\overline{(\mathit{Dom}\,(T_{LTL}(\mathbf{true}))\,;\rho)^*;\mathbf{tr};\overline{T_{LTL}(\neg\alpha_i \vee \neg I \vee \oplus(\neg\beta_i \vee I))}}\right)\,;\rho^* & \\
 & \text{(by def. } T_{LTL}\text{)} \\
\leq \mathbf{tr_0}\,;\mathit{Dom}\left(\mathbf{tr};\overline{(\mathbf{tr};\rho)^*;\mathbf{tr};\overline{T_{LTL}(\neg\alpha_i \vee \neg I \vee \oplus(\neg\beta_i \vee I))}}\right)\,;\rho^* & \\
 & \text{(by } \mathbf{tr} \leq \mathit{Dom}\,(T_{LTL}(\mathbf{true}))\text{)} \\
= \mathbf{tr_0}\,;\mathbf{tr}\,;\mathit{Dom}\left(\overline{(\mathbf{tr};\rho)^*;\mathbf{tr};\overline{T_{LTL}(\neg\alpha_i \vee \neg I \vee \oplus(\neg\beta_i \vee I))}}\right)\,;\rho^* & \text{(by Lemma A.1.4)} \\
= \mathbf{tr_0}\,;\mathit{Dom}\left(\overline{(\mathbf{tr};\rho)^*;\mathbf{tr};\overline{T_{LTL}(\neg\alpha_i \vee \neg I \vee \oplus(\neg\beta_i \vee I))}}\right)\,;\mathbf{tr};\rho^* & \text{(by Thm. A.2.5)}
\end{array}$$

Notice that $\mathit{Ran}\,(\mathbf{tr};\rho) \leq \mathbf{tr}$ by Lemma D.4,

$$\begin{array}{ll}
= \mathbf{tr_0}\,;\mathit{Dom}\left(\overline{(\mathbf{tr};\rho)^*;\mathbf{tr};\overline{T_{LTL}(\neg\alpha_i \vee \neg I \vee \oplus(\neg\beta_i \vee I))}}\right)\,;\mathbf{tr};\rho^*;\mathbf{tr} & \text{(by Lemma A.3)} \\
= \mathbf{tr_0}\,;\mathit{Dom}\left(\overline{(\mathbf{tr};\rho)^*;\mathbf{tr};\overline{T_{LTL}(\neg\alpha_i \vee \neg I \vee \oplus(\neg\beta_i \vee I))}}\right)\,;\mathbf{tr};(\mathbf{tr};\rho;\mathbf{tr})^*;\mathbf{tr} & \\
 & \text{(by Lemma A.3)} \\
\leq \mathbf{tr_0}\,;\mathit{Dom}\left(\overline{(\mathbf{tr};\rho)^*;\mathbf{tr};\overline{T_{LTL}(\neg\alpha_i \vee \neg I \vee \oplus(\neg\beta_i \vee I))}}\right)\,;(\mathbf{tr};\rho)^*;\mathbf{tr} & \\
 & \text{(by Thm. A.2.8 and monotonicity)} \\
\leq \mathbf{tr_0}\,;(\mathbf{tr};\rho)^*;\mathbf{tr};\mathit{Dom}\,(T_{LTL}(\neg\alpha_i \vee \neg I \vee \oplus(\neg\beta_i \vee I))) & \text{(by Lemma A.1.12)}
\end{array}$$

$$= \mathbf{tr_0};(\mathbf{tr};\rho)^*;Dom\begin{pmatrix} \mathbf{tr};\overline{T_{LTL}(\alpha_i)} \\ +\mathbf{tr};\overline{T_{LTL}(I)} \\ +\rho;(\mathbf{tr};\overline{T_{LTL}(\beta_i)+T_{LTL}(I)}) \end{pmatrix} \qquad \text{(by def. } T_{LTL}\text{)}$$

$$\leq \mathbf{tr_0};\rho^*;Dom\begin{pmatrix} \mathbf{tr};\overline{T_{LTL}(\alpha_i)} \\ +\mathbf{tr};\overline{T_{LTL}(I)} \\ +\rho;(\mathbf{tr};\overline{T_{LTL}(\beta_i)+T_{LTL}(I)}) \end{pmatrix}$$

(by Thm.A.2.8 and monotonicity)

$$= \mathbf{tr_0};\rho^*;Dom\begin{pmatrix} \mathbf{tr};\overline{T_{LTL}(\alpha_i)} \\ +\mathbf{tr};\overline{T_{LTL}(I)} \\ +\rho;\mathbf{tr};\overline{T_{LTL}(\beta_i)} \\ +\rho;\overline{T_{LTL}(I)} \end{pmatrix} \qquad \text{(by Lemma A.1.13)}$$

$$= \mathbf{tr_0};\rho^*;\begin{pmatrix} Dom\left(\mathbf{tr};\overline{T_{LTL}(\alpha_i)}\right) \\ +Dom\left(\mathbf{tr};\overline{T_{LTL}(I)}\right) \\ +Dom\left(\rho;\mathbf{tr};\overline{T_{LTL}(\beta_i)}\right) \\ +Dom\left(\rho;T_{LTL}(I)\right) \end{pmatrix} \qquad \text{(by Thm. A.1.12)}$$

$$= \mathbf{tr_0};\rho^*;\begin{pmatrix} \mathbf{tr};\neg Dom\left(T_{LTL}(\alpha_i)\right) \\ +\mathbf{tr};\neg Dom\left(T_{LTL}(I)\right) \\ +Dom\left(\rho;\mathbf{tr};\overline{T_{LTL}(\beta_i)}\right) \\ +Dom\left(\rho;T_{LTL}(I)\right) \end{pmatrix} \qquad \text{(by Thm. A.3.2 and Lemma A.1.4)}$$

Hence,

$$\mathbf{tr}_{\mathbf{0}}^{\rightarrow} = Ran\left(\mathbf{tr_0};\rho^*\right) \qquad \text{(by def. } \mathbf{tr}_{\mathbf{0}}^{\rightarrow}\text{)}$$

$$\leq Ran\left(\mathbf{tr_0};\rho^*;\begin{pmatrix} \mathbf{tr};\neg Dom\left(T_{LTL}(\alpha_i)\right) \\ +\mathbf{tr};\neg Dom\left(T_{LTL}(I)\right) \\ +Dom\left(\rho;\mathbf{tr};\overline{T_{LTL}(\beta_i)}\right) \\ +Dom\left(\rho;T_{LTL}(I)\right) \end{pmatrix}\right)$$

(by (4) and monotonicity of *Ran*)

$$= Ran\left(\mathbf{tr_0};\rho^*\right);\begin{pmatrix} \mathbf{tr};\neg Dom\left(T_{LTL}(\alpha_i)\right) \\ +\mathbf{tr};\neg Dom\left(T_{LTL}(I)\right) \\ +Dom\left(\rho;\mathbf{tr};\overline{T_{LTL}(\beta_i)}\right) \\ +Dom\left(\rho;T_{LTL}(I)\right) \end{pmatrix} \qquad \text{(by Lemma A.1.4)}$$

$$\leq \begin{pmatrix} \mathbf{tr};\neg Dom\left(T_{LTL}(\alpha_i)\right) \\ +\mathbf{tr};\neg Dom\left(T_{LTL}(I)\right) \\ +Dom\left(\rho;\mathbf{tr};\overline{T_{LTL}(\beta_i)}\right) \\ +Dom\left(\rho;T_{LTL}(I)\right) \end{pmatrix} \qquad \text{(by Thm. A.2.8)}$$

■

We will reduce notation by denoting relation $Ran\left(\pi \nabla (\mathbf{A_i} \otimes \rho)\right)$ as $Rg(\mathbf{A_i})$.

Lemma 6.3

$$\begin{array}{l} \textit{For all } i \in \mathcal{A}, \\ \mathbf{A_i} = Dom\,(T_{PDL}(\alpha_i))\,;\mathbf{A_i};Dom\,(T_{PDL}(\beta_i))\,, \\ \mathbf{tr}_{\mathbf{0}}^{\rightarrow} \leq \left(\begin{array}{l} \neg Dom\,(T_{LTL}(\alpha_i)) \\ +\neg Dom\,(T_{LTL}(I)) \\ +Dom\left(\rho;\mathbf{tr};\overline{T_{LTL}(\beta_i)}\right) \\ +Dom\,(\rho;T_{LTL}(I)) \end{array} \right) \end{array}$$

$\vdash_{\omega\text{-CCFA}^+}$

$$\begin{array}{l} \textit{For all } P \in PrgDLTL(\Sigma), \\ \begin{array}{lcl} \mathbf{tr_0};Dom\,(T_{DLTL}\,(I')) & \leq & \mathbf{tr_0};Dom\,(T_{DLTL}\,(I')) \\ ;M_{DLTL}(\mathbf{true},P) & & ;M_{DLTL}(I',P);Dom\,(T_{DLTL}\,(I')) \end{array} \end{array}$$

Proof. In order to prove this property, we will show that

$$\begin{array}{lcl} \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{DLTL}\,(I')) & \leq & \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{DLTL}\,(I')) \\ ;M_{DLTL}(\mathbf{true},P) & & ;M_{DLTL}(I',P);\mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{DLTL}\,(I')) \end{array} \tag{5}$$

- $P = a_i$

$$\begin{array}{ll} \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{DLTL}\,(I'))\,;M_{DLTL}(\mathbf{true},a_i) & \\ = \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{DLTL}\,(I'))\,;Dom\,(T_{DLTL}\,(\mathbf{true}))\,;Rg(\mathbf{A_i});\rho & \\ & \text{(by def. } M_{DLTL}\text{)} \\ \leq \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{DLTL}\,(I'))\,;Rg(\mathbf{A_i});\rho & \text{(by Thm.A.2.8)} \\ = \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{DLTL}\,(I')) & \\ \quad ;Rg(Dom\,(T_{PDL}(\alpha_i))\,;\mathbf{A_i};Dom\,(T_{PDL}(\beta_i)));\rho & \text{(by Hyp.)} \\ = \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{DLTL}\,(I'))\,;Rg(\mathbf{A_i}) & \\ \quad ;(Dom\,(T_{PDL}(\alpha_i))\otimes 1');\rho;(Dom\,(T_{PDL}(\beta_i))\otimes 1') & \\ & \text{(by Lemma A.2.5)} \\ = \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{DLTL}\,(I'))\,;Rg(\mathbf{A_i}) & \\ \quad ;Dom\,(\pi;T_{PDL}(\alpha_i))\,;\rho;Dom\,(\pi;T_{PDL}(\beta_i)) & \text{(by Thm. A.4.16)} \\ = \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{DLTL}\,(I'))\,;Rg(\mathbf{A_i}) & \\ \quad ;\mathbf{tr};Dom\,(\pi;T_{PDL}(\alpha_i))\,;\rho;\mathbf{tr};Dom\,(\pi;T_{PDL}(\beta_i)) & \\ & \text{(by Thms. A.2.5 and A.2.7 and Lemma D.4)} \\ = \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{DLTL}\,(I'))\,;Rg(\mathbf{A_i}) & \\ \quad ;Dom\,(\mathbf{tr};\pi;T_{PDL}(\alpha_i))\,;\rho;Dom\,(\mathbf{tr};\pi;T_{PDL}(\beta_i)) & \\ & \text{(by Lemma A.1.4)} \end{array}$$

$$
\begin{aligned}
&= \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; Rg(\mathbf{A_i}) \\
&\quad ; Dom\,(\mathbf{tr} ; T_{LTL}(\alpha_i)) \,; \rho ; Dom\,(\mathbf{tr} ; T_{LTL}(\beta_i)) && \text{(by Lemma D.9)} \\
&= \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; Rg(\mathbf{A_i}) \\
&\quad ; \mathbf{tr} ; Dom\,(T_{LTL}(\alpha_i)) \,; \rho ; \mathbf{tr} ; Dom\,(T_{LTL}(\beta_i)) && \text{(by Lemma A.1.4)} \\
&= \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{LTL}(I)) \,; Rg(\mathbf{A_i}) \\
&\quad ; \mathbf{tr} ; Dom\,(T_{LTL}(\alpha_i)) \,; \rho ; \mathbf{tr} ; Dom\,(T_{LTL}(\beta_i)) && \text{(by Lemma D.8)} \\
&\leq \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{LTL}(I)) \,; Rg(\mathbf{A_i}) \\
&\quad ; Dom\,(T_{LTL}(\alpha_i)) \,; \rho ; Dom\,(T_{LTL}(\beta_i)) && \text{(by monotonicity)} \\
&= \mathbf{tr}_0^{\rightarrow} ; \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{LTL}(I)) \,; Rg(\mathbf{A_i}) \\
&\quad ; Dom\,(T_{LTL}(\alpha_i)) \,; \rho ; Dom\,(T_{LTL}(\beta_i)) && \text{(by Thm. A.2.7)} \\
&\leq \mathbf{tr}_0^{\rightarrow} ; \begin{pmatrix} \neg Dom\,(T_{LTL}(\alpha_i)) \\ + \neg Dom\,(T_{LTL}(I)) \\ + Dom\left(\rho ; \mathbf{tr} ; \overline{T_{LTL}(\beta_i)}\right) \\ + Dom\,(\rho ; T_{LTL}(I)) \end{pmatrix} ; Dom\,(T_{LTL}(I)) \\
&\quad ; Rg(\mathbf{A_i}) ; Dom\,(T_{LTL}(\alpha_i)) \,; \rho ; Dom\,(T_{LTL}(\beta_i)) \\
& && \text{(by Hyp. and monotonicity)}
\end{aligned}
$$

Now, let us apply Ax. 2 and Lemma A.1.13 and label each relation.

$$
\begin{gathered}
\underbrace{\begin{array}{l} \mathbf{tr}_0^{\rightarrow} ; \neg Dom\,(T_{LTL}(\alpha_i)) \,; Dom\,(T_{LTL}(I)) \,; Rg(\mathbf{A_i}) \\ ; Dom\,(T_{LTL}(\alpha_i)) \,; \rho ; Dom\,(T_{LTL}(\beta_i)) \end{array}}_{r_1} \\
+ \\
\underbrace{\begin{array}{l} \mathbf{tr}_0^{\rightarrow} ; \neg Dom\,(T_{LTL}(I)) \,; Dom\,(T_{LTL}(I)) \,; Rg(\mathbf{A_i}) \\ ; Dom\,(T_{LTL}(\alpha_i)) \,; \rho ; Dom\,(T_{LTL}(\beta_i)) \end{array}}_{r_2} \\
+ \\
\underbrace{\begin{array}{l} \mathbf{tr}_0^{\rightarrow} ; Dom\left(\rho ; \mathbf{tr} ; \overline{T_{LTL}(\beta_i)}\right) ; Dom\,(T_{LTL}(I)) \,; Rg(\mathbf{A_i}) \\ ; Dom\,(T_{LTL}(\alpha_i)) \,; \rho ; Dom\,(T_{LTL}(\beta_i)) \end{array}}_{r_3} \\
+ \\
\underbrace{\begin{array}{l} \mathbf{tr}_0^{\rightarrow} ; Dom\,(\rho ; T_{LTL}(I)) \,; Dom\,(T_{LTL}(I)) \,; Rg(\mathbf{A_i}) \\ ; Dom\,(T_{LTL}(\alpha_i)) \,; \rho ; Dom\,(T_{LTL}(\beta_i)) \end{array}}_{r_4}
\end{gathered}
$$

Let us analyze relations r_1, r_2 ,r_3 and r_4 one at a time. For relation r_1,

$$
\begin{aligned}
& \mathbf{tr}_0^{\rightarrow} ; \neg Dom\,(T_{LTL}(\alpha_i)) \,; Dom\,(T_{LTL}(I)) \\
& \quad ; Rg(\mathbf{A_i}) ; Dom\,(T_{LTL}(\alpha_i)) \,; \rho ; Dom\,(T_{LTL}(\beta_i)) \\
& \leq \neg Dom\,(T_{LTL}(\alpha_i)) \,; Dom\,(T_{LTL}(\alpha_i)) \,; \rho && \text{(by Thm. A.2.8)} \\
& = (\neg Dom\,(T_{LTL}(\alpha_i)) \cdot Dom\,(T_{LTL}(\alpha_i))) ; \rho && \text{(by Thm. A.1.7)} \\
& = 0 && \text{(by Thm. A.3.3)}
\end{aligned}
$$

Regarding relation r_2, a proof similar to the one performed for r_1 allows us to show that

$$\begin{array}{l}\mathbf{tr}_{\mathbf{0}}^{\rightarrow};\neg Dom\,(T_{LTL}(I))\,;Dom\,(T_{LTL}(I))\,;Rg(\mathbf{A}_{\mathrm{i}})\\ \quad;Dom\,(T_{LTL}(\alpha_i))\,;\rho;Dom\,(T_{LTL}(\beta_i))\end{array} = 0$$

Regarding relation r_3,

$$\begin{aligned}
&\mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\left(\rho;\mathbf{tr};\overline{T_{LTL}(\beta_i)}\right);Dom\,(T_{LTL}(I))\,;Rg(\mathbf{A}_{\mathrm{i}})\\
&\quad;Dom\,(T_{LTL}(\alpha_i))\,;\rho;Dom\,(T_{LTL}(\beta_i))\\
&\leq Dom\left(\rho;\overline{T_{LTL}(\beta_i)}\right);\rho;Dom\,(T_{LTL}(\beta_i)) && \text{(by Thm. A.2.8)}\\
&= \rho;Dom\left(\overline{T_{LTL}(\beta_i)}\right);Dom\,(T_{LTL}(\beta_i)) && \text{(by Lemma A.1.5)}\\
&= \rho;\left(Dom\left(\overline{T_{LTL}(\beta_i)}\right)\cdot Dom\,(T_{LTL}(\beta_i))\right) && \text{(by Thm. A.1.7)}\\
&= 0 && \text{(by Thm. A.3.3)}
\end{aligned}$$

And finally, from r_4 we have that,

$$\begin{aligned}
&\mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(\rho;T_{LTL}(I))\,;Dom\,(T_{LTL}(I))\\
&\quad;Rg(\mathbf{A}_{\mathrm{i}});Dom\,(T_{LTL}(\alpha_i))\,;\rho;Dom\,(T_{LTL}(\beta_i))\\
&\leq \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(\rho;T_{LTL}(I))\,;Dom\,(T_{LTL}(I))\,;Rg(\mathbf{A}_{\mathrm{i}});\rho \quad \text{(by Thm. A.2.8)}\\
&= \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{LTL}(I))\,;Rg(\mathbf{A}_{\mathrm{i}});Dom\,(\rho;T_{LTL}(I))\,;\rho \quad \text{(by Thm. A.2.5)}\\
&= \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{LTL}(I))\,;Rg(\mathbf{A}_{\mathrm{i}});\rho;Dom\,(T_{LTL}(I)) \quad \text{(by Lemma A.1.5)}\\
&= \mathbf{tr}_{\mathbf{0}}^{\rightarrow};\mathbf{tr};Dom\,(T_{LTL}(I))\,;Rg(\mathbf{A}_{\mathrm{i}});\rho;Dom\,(T_{LTL}(I))\\
&\qquad \text{(by Lemma D.10)}\\
&= \mathbf{tr}_{\mathbf{0}}^{\rightarrow};\mathbf{tr};Dom\,(T_{LTL}(I))\,;Rg(\mathbf{A}_{\mathrm{i}});\mathbf{tr};\rho;Dom\,(T_{LTL}(I))\\
&\qquad \text{(by Thms. A.2.7 and A.2.5)}\\
&= \mathbf{tr}_{\mathbf{0}}^{\rightarrow};\mathbf{tr};Dom\,(T_{LTL}(I))\,;Rg(\mathbf{A}_{\mathrm{i}});\mathbf{tr};\rho;\mathbf{tr};Dom\,(T_{LTL}(I))\\
&\qquad \text{(by Lemma D.4)}\\
&\leq \mathbf{tr}_{\mathbf{0}}^{\rightarrow};\mathbf{tr};Dom\,(T_{LTL}(I))\,;Rg(\mathbf{A}_{\mathrm{i}});\rho;\mathbf{tr};Dom\,(T_{LTL}(I))\\
&\qquad \text{(by Thm. A.2.8)}\\
&= \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(\mathbf{tr};T_{LTL}(I))\,;Rg(\mathbf{A}_{\mathrm{i}});\rho;Dom\,(\mathbf{tr};T_{LTL}(I))\\
&\qquad \text{(by Lemma A.1.4)}\\
&= \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(\mathbf{tr};T_{DLTL}\,(I'))\,;Rg(\mathbf{A}_{\mathrm{i}});\rho;Dom\,(\mathbf{tr};T_{DLTL}\,(I'))\\
&\qquad \text{(by Lemma D.8 and def. } I')\\
&\leq \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{DLTL}\,(I'))\,;Rg(\mathbf{A}_{\mathrm{i}});\rho;Dom\,(T_{DLTL}\,(I'))\\
&\qquad \text{(by Thm. A.2.8 and monotonicity of } Dom)\\
&= \mathbf{tr}_{\mathbf{0}}^{\rightarrow};Dom\,(T_{DLTL}\,(I'))\,;Rg(\mathbf{A}_{\mathrm{i}});\mathbf{tr}_{\mathbf{0}}^{\rightarrow};\rho;Dom\,(T_{DLTL}\,(I'))\\
&\qquad \text{(by Thms. A.2.7 and A.2.5)}
\end{aligned}$$

$$= \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; Rg(\mathbf{A_i}) ; \mathbf{tr}_0^{\rightarrow} ; \rho ; \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I'))$$
(by Lemma D.11)

$$\leq \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; Rg(\mathbf{A_i}) ; \rho ; \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I'))$$
(by Thm. A.2.8)

$$= \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; Dom\,(T_{DLTL}\,(I')) \,; Rg(\mathbf{A_i}) ; \rho ; \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I'))$$
(by Thm. A.2.7)

$$= \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(I', a_i) ; \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I'))$$
(by def. M_{DLTL})

- $P = Q \cup R$

$$\mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(\mathbf{true}, Q \cup R)$$

$$= \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; \left(\begin{array}{l} M_{DLTL}(\mathbf{true}, Q) \\ \quad + M_{DLTL}(\mathbf{true}, R) \end{array} \right)$$
(by def. M_{DLTL})

$$= \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(\mathbf{true}, Q) + \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(\mathbf{true}, R)$$
(by Lemma A.1.13)

$$\leq \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(I', Q) ; \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) + \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(I', R) ; \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I'))$$
(by Ind. Hyp.)

$$= \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; \left(\begin{array}{l} M_{DLTL}(I', Q) \\ + M_{DLTL}(I', R) \end{array} \right) ; \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I'))$$
(by Ax. 2 and Lemma A.1.13)

$$= \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(I', Q \cup R) ; \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I'))$$
(by def. M_{DLTL})

- $P = Q; R$

$$\mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(\mathbf{true}, Q; R)$$

$$= \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(\mathbf{true}, Q) ; M_{DLTL}(\mathbf{true}, R)$$
(by def. M_{DLTL})

$$\leq \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(I', Q) ; \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(\mathbf{true}, R)$$
(by Ind. Hyp.)

$$\leq \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(I', Q) ; \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(I', R) ; \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I'))$$
(by Ind. Hyp.)

$$\leq \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(I', Q) ; M_{DLTL}(I', R) ; \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I'))$$
(by Thm. A.2.8)

$$= \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I')) \,; M_{DLTL}(I', Q; R) ; \mathbf{tr}_0^{\rightarrow} ; Dom\,(T_{DLTL}\,(I'))$$
(by def. M_{DLTL})

- $P = Q^*$.
  We will begin by proving that the hypothesis of Lemma A.3 are satisfied. First, note that,

  $$Ran\,(\mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I'))\,;M_{DLTL}(\mathbf{true}, Q)) \leq \mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I')) \quad \text{(by Ind. Hyp.)}$$

  And we also have that,

  $$\mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I')) \leq 1'$$

  Then, once the hypothesis that allow the application of Lemma A.3 has been established, we proceed as follows:

  $$\begin{aligned}
  & \mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I'))\,;M_{DLTL}(\mathbf{true}, Q^*) \\
  &= \mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I'))\,;(M_{DLTL}(\mathbf{true}, Q))^* && \text{(by def. } M_{DLTL}) \\
  &= \mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I'))\,;(\mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I'))\,;M_{DLTL}(\mathbf{true}, Q))^* && \text{(by Lemma A.3)} \\
  &\leq \mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I')) \\
  &\quad ;(\mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I'))\,;M_{DLTL}(I', Q);\mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I')))^* && \text{(by Ind. Hyp.)} \\
  &= \mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I'))\,;(M_{DLTL}(I', Q))^*;\mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I')) && \text{(by Lemma A.3)} \\
  &= \mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I'))\,;M_{DLTL}(I', Q^*);\mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I')) && \text{(by def. } M_{DLTL})
  \end{aligned}$$

We finish this proof by showing that property holds,

$$\begin{aligned}
& \mathbf{tr}_0;Dom\,(T_{DLTL}\,(I'))\,;M_{DLTL}(\mathbf{true}, P) \\
&= \mathbf{tr}_0;\mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I'))\,;M_{DLTL}(\mathbf{true}, P) && \text{(since } \mathbf{tr}_0 \leq \mathbf{tr}_0^{\rightarrow}) \\
&\leq \mathbf{tr}_0;\mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I'))\,;M_{DLTL}(I', P);\mathbf{tr}_0^{\rightarrow}\,;Dom\,(T_{DLTL}\,(I')) && \text{(by (5))} \\
&\leq \mathbf{tr}_0;Dom\,(T_{DLTL}\,(I'))\,;M_{DLTL}(I', P);Dom\,(T_{DLTL}\,(I')) && \text{(by Thm. A.2.8)}
\end{aligned}$$

■

We continue by presenting Thm. 6.2 and its proof.

Theorem 6.2

For all $i \in \mathcal{A}$,
$\mathbf{S};T_{PDL}(\alpha_i \Longrightarrow [a_i]\beta_i) = \mathbf{S};\mathbf{1}$,
$\mathbf{S};T_{PDL}(\neg\alpha_i \Longrightarrow [a_i]\mathbf{false}) = \mathbf{S};\mathbf{1}$,
$\mathbf{tr}_0;T_{LTL}(\Box(\alpha_i \wedge I \Longrightarrow \oplus(\beta_i \Longrightarrow I))) = \mathbf{tr}_0;\mathbf{1}$

$\vdash_{\omega\text{-CCFA}^+}$

For all $P \in PrgDLTL(\Sigma)$,
$\mathbf{tr}_0;T_{DLTL}\left((\mathbf{true}\ \mathsf{U}^P\ \mathbf{true}) \Longrightarrow (I' \Longrightarrow (I'\ \mathsf{U}^P\ I'))\right) = \mathbf{tr}_0;\mathbf{1}$

Proof.

$\leq$)

$$\mathbf{tr_0}\,;T_{DLTL}\left((\mathbf{true}\ \mathsf{U}^P\ \mathbf{true}) \Longrightarrow (I' \Longrightarrow (I'\ \mathsf{U}^P\ I'))\right) \leq \mathbf{tr_0}\,;\mathbf{1}$$
(by monotonicity)

$\geq$) In order to prove the inclusion, we will show that

$$\mathbf{tr_0}\,;T_{DLTL}\left(\mathbf{true}\ \mathsf{U}^P\ \mathbf{true}\right) \leq \mathbf{tr_0}\,;T_{DLTL}\left(I' \Longrightarrow (I'\ \mathsf{U}^P\ I')\right) \quad (6)$$

We proceed as follows,

$$\begin{aligned}
& \mathbf{tr_0}\,;T_{DLTL}\left(\mathbf{true}\ \mathsf{U}^P\ \mathbf{true}\right) \\
&= \mathbf{tr_0}\,;M_{DLTL}(\mathbf{true}, P);T_{DLTL}\left(\mathbf{true}\right) && \text{(by def. } T_{DLTL}) \\
&\leq \mathbf{tr_0}\,;M_{DLTL}(\mathbf{true}, P);\mathbf{1} && \text{(by monotonicity)} \\
&= \mathbf{tr_0}\,;\mathbf{tr}\,;M_{DLTL}(\mathbf{true}, P);\mathbf{1} && \text{(by Lemma D.15)} \\
&= \mathbf{tr_0}\,;\mathbf{tr}\,;M_{DLTL}(\mathbf{true}, P);\mathbf{tr}\,;\mathbf{1} && \text{(by Lemma D.5)} \\
&= \mathbf{tr_0}\,;\mathit{Dom}\left(T_{DLTL}\left(I'\right)\right);\mathbf{tr}\,;M_{DLTL}(\mathbf{true}, P);\mathbf{tr}\,;\mathbf{1} \\
&\quad +\mathbf{tr_0}\,;\neg\mathit{Dom}\left(T_{DLTL}\left(I'\right)\right);\mathbf{tr}\,;M_{DLTL}(\mathbf{true}, P);\mathbf{tr}\,;\mathbf{1} \\
& && \text{(by Thm. A.2.9)} \\
&\leq \mathbf{tr_0}\,;\mathit{Dom}\left(T_{DLTL}\left(I'\right)\right);\mathbf{tr}\,;M_{DLTL}(I', P);\mathit{Dom}\left(T_{DLTL}\left(I'\right)\right);\mathbf{tr}\,;\mathbf{1} \\
&\quad +\mathbf{tr_0}\,;\neg\mathit{Dom}\left(T_{DLTL}\left(I'\right)\right);\mathbf{tr}\,;M_{DLTL}(\mathbf{true}, P);\mathbf{tr}\,;\mathbf{1} \\
& && \text{(by Lemma 6.3)} \\
&= \mathbf{tr_0}\,;\mathit{Dom}\left(T_{DLTL}\left(I'\right)\right);\mathbf{tr}\,;M_{DLTL}(I', P);\mathit{Dom}\left(T_{DLTL}\left(I'\right)\right);\mathbf{tr}\,;\mathbf{1} \\
&\quad +\mathbf{tr_0}\,;\neg\mathit{Dom}\left(T_{DLTL}\left(I'\right)\right);\mathit{Dom}\left(\mathbf{tr}\,;M_{DLTL}(\mathbf{true}, P);\mathbf{tr}\right);\mathbf{1} \\
& && \text{(by Thm. A.1.14)} \\
&\leq \mathbf{tr_0}\,;M_{DLTL}(I', P);\mathit{Dom}\left(T_{DLTL}\left(I'\right)\right);\mathbf{1} \\
&\quad +\mathbf{tr_0}\,;\neg\mathit{Dom}\left(T_{DLTL}\left(I'\right)\right);\mathbf{1} && \text{(by Thm. A.2.8)} \\
&= \mathbf{tr_0}\,;M_{DLTL}(I', P);\mathit{Dom}\left(T_{DLTL}\left(I'\right)\right);\mathbf{1} \\
&\quad +\mathbf{tr_0}\,;\mathit{Dom}\left(\overline{T_{DLTL}\left(I'\right)}\right);\mathbf{1} && \text{(by Thm. A.3.2)} \\
&= \mathbf{tr_0}\,;M_{DLTL}(I', P);T_{DLTL}\left(I'\right);\mathbf{1}+\mathbf{tr_0}\,;\overline{T_{DLTL}\left(I'\right)};\mathbf{1} \\
& && \text{(by Thm. A.1.14)} \\
&= \mathbf{tr_0}\,;M_{DLTL}(I', P);T_{DLTL}\left(I'\right)+\mathbf{tr_0}\,;\overline{T_{DLTL}\left(I'\right)} \\
& && \text{(by } T_{DLTL} \text{ and } \overline{T_{DLTL}} \text{ right ideals)}
\end{aligned}$$

$$= \mathbf{tr_0};M_{DLTL}(I',P);T_{DLTL}(I') + \mathbf{tr_0};\mathbf{tr};\overline{T_{DLTL}(I')}$$
(by Lemma D.15)
$$= \mathbf{tr_0};\left(M_{DLTL}(I',P);T_{DLTL}(I') + \mathbf{tr};\overline{T_{DLTL}(I')}\right)$$
(by Lemma A.1.13)
$$= \mathbf{tr_0};T_{DLTL}\left(I' \Longrightarrow I' \mathsf{U}^P I'\right) \quad \text{(by def. } T_{DLTL}\text{)}$$

Therefore,

$$\mathbf{tr_0};T_{DLTL}\left((\mathbf{true}\ \mathsf{U}^P\ \mathbf{true}) \Longrightarrow (I' \Longrightarrow (I' \mathsf{U}^P I'))\right)$$
$$= \mathbf{tr_0};(\mathbf{tr};\overline{T_{DLTL}(\mathbf{true}\ \mathsf{U}^P\ \mathbf{true})} + T_{DLTL}\left(I' \Longrightarrow I' \mathsf{U}^P I'\right))$$
(by def. T_{DLTL})
$$= \mathbf{tr_0};\mathbf{tr};\overline{T_{DLTL}(\mathbf{true}\ \mathsf{U}^P\ \mathbf{true})} + \mathbf{tr_0};T_{DLTL}\left(I' \Longrightarrow I' \mathsf{U}^P I'\right)$$
(by Lemma A.1.13)
$$= \mathbf{tr_0};\overline{T_{DLTL}(\mathbf{true}\ \mathsf{U}^P\ \mathbf{true})} + \mathbf{tr_0};T_{DLTL}\left(I' \Longrightarrow I' \mathsf{U}^P I'\right)$$
(by Lemma D.15)
$$\geq \mathbf{tr_0};\overline{T_{DLTL}(\mathbf{true}\ \mathsf{U}^P\ \mathbf{true})} + \mathbf{tr_0};T_{DLTL}\left(\mathbf{true}\ \mathsf{U}^P\ \mathbf{true}\right) \quad \text{(by (6))}$$
$$= \mathbf{tr_0};(\overline{T_{DLTL}(\mathbf{true}\ \mathsf{U}^P\ \mathbf{true})} + T_{DLTL}\left(\mathbf{true}\ \mathsf{U}^P\ \mathbf{true}\right))$$
(by Lemma A.1.13)
$$= \mathbf{tr_0};\mathbf{1} \quad \text{(BA)}$$

■

7 Case-Study: A Fictitious Mobile Tourist Information Guide

In this section we present a case-study of verification of properties using fork algebras. This case-study shows a fictitious system that is a instance of the abstract system showed in subsection 6.1.

In subsection 7.1 we present a brief introduction to our case-study (both system features and desirable property). In subsection 7.2 we give a detailed description of such a system through natural language. In subsection 7.3 we define the collection of atomic propositions that will serve to keep track of system state. In subsection 7.4 we show dynamic behavior as a instance of the *specPDL* theory. In the same way, in subsection 7.5 we show linear temporal behavior as a instance of the *specLTL* theory. Finally, in subsection 7.6, we end the case-study presentation by concluding that system meets the desirable property.

7.1 Introduction

A user of a mobile system interacts with the system while on the road. Think for instance of a tourist with his PDA[2] in a city, interacting with some local information server through a wireless connection.

Once tourist has logged into the system, his PDA signals every change of position automatically (with no need of human interaction).

Some of the interactions can be influenced by the tourist location. As an example, asking for hotels to spend the night, might retrieve the hotels in the zone (say ten blocks around). Similarly, asking for cash dispensers will result in the nearest cash dispensers in the zone. Any time he changes his position, all previously gathered location-sensitive information becomes useless, and it can be erased from his PDA.

Now, the verification engineers wish to ensure that, if a local server reaches proper behavior, it remains invariant along any execution of the server.

7.2 The Fictitious Mobile Tourist Information Guide

Once user becomes a member of the *Mobile Tourist Information Guide* service, he is able to log into the system if user location falls within geographical coverage.

- Due to its low computational cost, a local server can perform either a user-login or a user-logout almost instantaneously.
- After user logs in, his PDA reports his actual position. Depending on local server load, this position report can be immediately served (updating user current position) or enqueued for further processing.

[2] Personal digital assistant, a handheld device that combines computing, telephone/fax, Internet and networking features.

- Following position report, a user may request for location-sensitive information on a variety of topics, such as hotels, restaurants, cash dispensers, etc.

- Any request of location-sensitive information involves a high computational cost (i.e.: queries on both internal and external databases, fetching data from internet, conducting searches in federative systems, etc.). Therefore, these requests can be either enqueued or served.

- System protocols ensure that every server delivers location-sensitive information according to current user position. In other words, a user never receives location-sensitive information belonging to a sector different from where he is.

- Queue policy implementation assures abscence of starvation for user requests.

- User receives location-sensitive advertising at least once a session.

- City space is divided into discrete sectors (e.g.: honeycombs in cellular phone technology), and each covered city has a unique local server.

7.3 System States

Due to the limited network bandwidth and data-retrieval capability, only a finite number of users can connect simultaneously to a unique server. We model this fact by defining a finite set $\mathcal{U}$ of possible user connections.

In the same way, we model city space as a discrete fixed set $\mathcal{S}$ of sectors. Also, we limit the location-sensitive information topics to a finite set $\mathcal{I}$.

Therefore, given a covered city, we capture system state through a finite set of atomics propositions:

- $\mathbf{logged}_u$, asserts that user u is logged into the system,

- $\mathbf{position}_{u,s}$, asserts that position s is the current position of user u,

- $\mathbf{localInfo}_{u,s,i}$, asserts that user u has received location-sensitive information on topic i in position s,

- $\mathbf{advertising}_{u,s,i}$, asserts that server has sent user u advertising of topic i in position s,

- $\mathbf{pndngUpdtPos}_{u,s}$, asserts that PDA of user u has reported a new position s, but server has enqueued the update,

- $\mathbf{pndngRtrvLclInfo}_{u,i}$, asserts that user u has requested location-sensitive information on topic i, but server has enqueued the request.

7.4 System Dynamic Behavior

Both user and server can trigger *actions* (i.e.: requesting location-sensitive information, serving enqueued requests, etc.). Actions might lead to a transition between different system states.

We formalize these actions together with its pre and post conditions using a instance of theory *specPDL* defined in 6.1.

In other words, we enumerate the components of formulas of the shape:

$$\alpha_i \Longrightarrow [a_i]\beta_i, \text{ for all } i \in \mathcal{A},$$
$$(\neg\alpha_i) \Longrightarrow [a_i]\mathbf{false}, \text{ for all } i \in \mathcal{A}.$$

Now, let u,$u' \in \mathcal{U}$, s,$s' \in \mathcal{S}$, and let $i \in \mathcal{I}$.

- user u begins a session,

$$\begin{aligned} \alpha_1 &= \neg\mathbf{logged}_u \\ a_1 &= \mathit{Login}_u \\ \beta_1 &= \mathbf{logged}_u \end{aligned}$$

- user u ends a session,

$$\begin{aligned} \alpha_2 &= \mathbf{logged}_u \\ a_2 &= \mathit{Logout}_u \\ \beta_2 &= \neg\mathbf{logged}_u \end{aligned}$$

- PDA of user u reports a new position s,

$$\begin{aligned} \alpha_3 &= \mathbf{logged}_u \\ a_3 &= \mathit{ReportPos}_{u,s} \\ \beta_3 &= \bigwedge_{\substack{i \in \mathcal{I} \\ s' \in \mathcal{U} \\ s' \neq s}} \neg\mathbf{localInfo}_{u,s',i} \wedge \\ & \left(\left(\mathbf{position}_{u,s} \wedge \bigwedge_{\substack{s' \in \mathcal{U} \\ s' \neq s}} \neg\mathbf{position}_{u,s'} \right) \vee \mathbf{pndngUpdtPos}_{u,s} \right) \end{aligned}$$

- user u requests for some local information i,

$$\begin{aligned} \alpha_4 &= \mathbf{logged}_u \wedge \mathbf{position}_{u,s} \bigwedge_{\substack{s' \in \mathcal{U} \\ s' \neq s}} \neg\mathbf{pndngUpdtPos}_{u,s'} \\ a_4 &= \mathit{RetrieveLocalInfo}_{u,i} \\ \beta_4 &= \mathbf{localInfo}_{u,s,i} \vee \mathbf{pndngRtrvLclInfo}_{u,i} \end{aligned}$$

- local server responses information request from user u,

$$\begin{aligned}
\alpha_5 &= \mathbf{logged}_u \wedge \mathbf{pndngRtrvLclInfo}_{u,i} \wedge \mathbf{position}_{u,s}\\
a_5 &= \mathit{SendInfo}_{u,i}\\
\beta_5 &= \mathbf{localInfo}_{u,s,i} \wedge \neg\mathbf{pndngRtrvLclInfo}_{u,i}
\end{aligned}$$

- local server attends a change of position from user u,

$$\begin{aligned}
\alpha_6 &= \mathbf{logged}_u \wedge \mathbf{position}_{u,s'} \wedge \mathbf{pndngUpdtPos}_{u,s}\\
a_6 &= \mathit{UpdatePosition}_{u,s}\\
\beta_6 &= \mathbf{position}_{u,s} \wedge \neg\mathbf{pndngUpdtPos}_{u,s} \wedge \neg\mathbf{position}_{u,s'}
\end{aligned}$$

- local server sends advertising to user u,

$$\begin{aligned}
\alpha_7 &= \mathbf{logged}_u \wedge \mathbf{localInfo}_{u,s,i}\\
a_7 &= \mathit{SendAd}_{u,i}\\
\beta_7 &= \mathbf{advertising}_{u,s,i}
\end{aligned}$$

7.5 System Linear Temporal Behavior

Finally, certain time concerning properties hold globally. As an example: *no user request can be enqueued indefinitely.* We specify such properties as a instance of theory *specLTL* defined in 6.2.

In other words, we will define a formula I such that,

$$\Box((\alpha_i \wedge I) \Longrightarrow \oplus(\beta_i \Longrightarrow I)), \text{ for all } i \in \mathcal{A}.$$

- Local server do not enqueue position updates indefinitely,

$$I_1 = \Box\left(\bigwedge_{\substack{u \in \mathcal{U}\\ s \in \mathcal{S}}} \mathbf{pndngUpdtPos}_{u,s} \Longrightarrow \Diamond\left(\begin{array}{l} (\mathbf{position}_{u,s} \wedge \neg\mathbf{pndngUpdtPos}_{u,s})\\ \vee\neg\mathbf{logged}_u \end{array}\right)\right)$$

- Local server do not enqueue requests of information indefinitely,

$$I_2 = \Box\left(\bigwedge_{\substack{i \in \mathcal{I}\\ u \in \mathcal{U}}} \mathbf{pndngRtrvLclInfo}_{u,i} \Longrightarrow \Diamond\left(\begin{array}{l} \bigwedge_{s \in \mathcal{S}} \left(\begin{array}{l} \mathbf{position}_{u,s}\\ \Longrightarrow \mathbf{localInfo}_{u,s,i} \end{array}\right)\\ \vee\neg\mathbf{logged}_u \end{array}\right)\right)$$

- Local server sends advertising to user at least once per session,

$$I_3 = \Box\left(\bigwedge_{u \in \mathcal{U}} \mathbf{logged}_u \Longrightarrow \mathbf{logged}_u \cup \mathit{advSent}_u \right)$$

where $advSent_u$ stands for formula:

$$\bigwedge_{s \in \mathcal{S}} \left(\textbf{position}_{u,s} \Longrightarrow \bigvee_{i \in \mathcal{I}} \textbf{advertising}_{u,s,i} \right)$$

- Each user eventually ends session,

$$I_4 = \Box \left(\bigwedge_{u \in \mathcal{U}} (\textbf{logged}_u \Longrightarrow \Diamond \neg \textbf{logged}_u) \right)$$

Using I_1, I_2, I_3 and I_4, we define formula I of *specLTL* theory as,

$$I = I_1 \wedge I_2 \wedge I_3 \wedge I_4$$

7.6 Verification of dynamic linear temporal properties

Since the *Mobile Tourist Information Guide* is a instance of *specPDL* and *specLTL* theories, and by reasoning presented in subsection 6.2, we can ensure that the desirable *PDLTL* property holds. In other words, system meets that,

> If a local server reaches proper behavior, this proper behavior remains invariant along any execution of the server.

8 Conclusions

We have presented a interpretability result for the dynamic linear temporal logic DLTL. Jointly with previous results on the interpretability of PDL and LTL, this allows us to propose a general framework for reasoning across dynamic and linear temporal logics. We use this framework to verify a non trivial property that combines both dynamic and linear temporal concepts. Finally, we presented a realistic problem in which such reasoning is relevant.

References

[Bar77] Jon Barwise, editor. *Handbook of Mathematical Logic.* North Holland, 1977.

[BFM98] Gabriel A. Baum, Marcelo F. Frias, and Tomas S. E. Maibaum. A logic for real-time systems specification, its algebraic semantics, and equational calculus. In Armando M. Haeberer, editor, *Proceedings of Algebraic Methodology And Software Technology*, volume 1548 of *Lecture Notes in Computer Science*, pages 91–105, Amazonia, Brasil, January 1998. Springer-Verlag.

[BS81] Stanley Burris and H. P. Sankappanavar. *A course in universal algebra.* Graduate Texts in Mathematics. Springer-Verlag, 1981.

[CT51] Louise H. Chin and Alfred Tarski. Distributive and modular laws in the arithmetic of relation algebras. *University of California Publications in Mathematics*, New Series(1):341–384, 1951.

[dM66] A. de Morgan. *On the syllogism, and other logical writings.* Yale University Press, 1966.

[Eme90] E. Allen Emerson. Temporal and modal logic. In Jan van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B. Elsevier, Amsterdam, 1990.

[FBHV95] Marcelo F. Frias, Gabriel A. Baum, Armando M. Haeberer, and Paulo A. S. Veloso. Fork algebras are representable. *Bulletin of the Section of Logic*, 24(2):64–75, 1995.

[FBM01] Marcelo F. Frias, Gabriel A. Baum, and Tomas S. E. Maibaum. Interpretability of first-order dynamic logic in a relational calculus. In Harrie de Swart, editor, *Proceedings of the 6th. Conference on Relational Methods in Computer Science (RelMiCS) - TARSKI*, pages 66–80, Oisterwijk, The Netherlands, October 2001.

[FHV97] Marcelo F. Frias, Armando M. Haeberer, and Paulo A. S. Veloso. A finite axiomatization for fork algebras. *Logic Journal of the IGPL*, 5(3):311–319, 1997.

[FO98] Marcelo F. Frias and Ewa Orlowska. Equational reasoning in non-classical logics. *Journal of Applied Non-classical Logics*, 8(1–2):27–66, 1998.

[FP] Marcelo F. Frias and Carlos G. Lopez Pombo. Interpretability of first-order linear temporal logics in fork algebras. *Journal of Logic and Algebraic Programming*. in press.

[FP03] Marcelo F. Frias and Carlos G. Lopez Pombo. Time is on my side. In Rudolf Berghammer and Bernhard Möller, editors, *Proceedings of the 7th. Conference on Relational Methods in Computer Science (RelMiCS) - 2nd. International Workshop on Applications of Kleene Algebra*, pages 105–111, Malente, Germany, May 2003.

[Fri02] Marcelo F. Frias. *Fork algebras in algebra, logic and computer science*. Logic and Computer Science. World Scientific Publishing Co., 2002.

[Gyu97] Viktor Gyuris. A short proof of representability of fork algebra. *Theoretical Computer Science*, 188(1–2):211–220, November 1997.

[HKT00] David Harel, Dexter Kozen, and J. Tiuryn. *Dynamic logic*. Foundations of Computing. MIT Press, 2000. ISBN: 0-262-08289-6.

[HT99] Jesper G. Henriksen and P.S. Thiagarajan. Dynamic linear time temporal logic. *Annals of Pure and Applied Logic*, 96(1–3):187–207, 1999.

[HV91] Armando M. Haeberer and Paulo A. S. Veloso. Partial relations for program derivation: adequacy, inevitability and expressiveness. In *Proceedings of the Working Conference on Constructing Programs from Specifications '91*, pages 310–352. IFIP TC2, Constructing Programs from Specifications, North Holland, 1991.

[JT52] Bjarni Jónnson and Alfred Tarski. Boolean algebra with operators, part II. *American Journal of Mathematics*, 74:127–162, 1952.

[Lyn50] R. Lyndon. The representation of relation algebras, part I. *Annals of Mathematics (series 2)*, 51(2):707–729, 1950.

[Pei33] Charles Sanders Peirce. *Collected Papers*. Harvard University Press, 1933.

[Sch95] E. F. W. K. Schöder. Vorlesungen, über die algebra der logik (exact logik). In *Algebra und Logik der Relative*, volume 3. Thoemmes Press, 1895.

[Tar41] Alfred Tarski. On the calculus of relations. *Journal of Symbolic Logic*, 6(3):73–89, September 1941.

[Tar55] Alfred Tarski. Contributions to the theory of models III. *Indagationes Mathematicae*, 17:56–64, 1955.

[TG87] Alfred Tarski and Steven Givant. *A formalization of Set Theory without Variables.* American Mathematical Society Colloqium Publications, 1987.

[VHF95] Paulo A. S. Veloso, Armando M. Haeberer, and Marcelo F. Frias. Fork algebras as algebras of logic. *Abstracts of the Logic Colloquium '94*, page 127, July 1995. Also in Bulletin of Symbolic Logic, 1(2):265–266, 1995.

A Arithmetical Properties of Omega Closure Fork Algebras

Theorem A.1 *The following properties are valid in all relation algebras for all relations R, S, T, F, G and I:*

1. $R;0 = 0;R = 0$.
2. $\breve{\mathbf{1}} = \mathbf{1}$.
3. $\mathbf{1};\mathbf{1} = \mathbf{1}$.
4. $(R+S)^{\smile} = \breve{R}+\breve{S}$.
5. $(R \cdot S)^{\smile} = \breve{R} \cdot \breve{S}$.
6. *If* $R \leq 1'$ *then* $\breve{R} = R$.
7. *If* $R, S \leq 1'$ *then* $R;S = R \cdot S$.
8. *If* $R \leq 1'$ *then* $(R;\mathbf{1}) \cdot S = R;S$ *and* $(\mathbf{1};R) \cdot S = S;R$.
9. *If* $F+G = 1'$ *and* $F \cdot G = 0$, *then* $\overline{F;\mathbf{1}} = G;\mathbf{1}$.
10. $Dom\,(R) = (R;\mathbf{1}) \cdot 1'$ *and* $Ran\,(R) = (\mathbf{1};R) \cdot 1'$.
11. $Dom\,(R)\,;R = R$ *and* $R;Ran\,(R) = R$.
12. $Dom\,(R+S) = Dom\,(R) + Dom\,(S)$, *i.e., Dom is additive. Similarly,* $Ran\,(R+S) = Ran\,(R) + Ran\,(S)$.
13. $Dom\left(\breve{R}\right) = Ran\,(R)$ *and* $Ran\left(\breve{R}\right) = Dom\,(R)$.
14. $R;\mathbf{1} = Dom\,(R)\,;\mathbf{1}$ *and* $\mathbf{1};R = \mathbf{1};Ran\,(R)$.
15. $\breve{\overline{R}} = \overline{\breve{R}}$.
16. $(R \cdot S)\,;T \leq (R;T) \cdot (S;T)$ *and* $R;(S \cdot T) \leq (R;S) \cdot (R;T)$.
17. *If F is a functional relation then* $F;(R \cdot S) = (F;R) \cdot (F;S)$.
18. *If F is a functional relation,* $G \leq F$, *and* $Dom\,(G) = Dom\,(F)$ *then* $G = F$.
19. *If F is a functional relation then* $Dom\,(F)\,;\overline{F;R} = F;\overline{R}$.
20. *If I is a injective relation then* $(R \cdot S)\,;I = (R;I) \cdot (S;I)$.
21. *If I is a injective relation then* $\overline{R;I};Ran\,(I) = \overline{R};I$.
22. *If* $F \leq 1'$ *then* $F;R \cdot S = F;(R \cdot S)$ *and* $R;F \cdot S = (R \cdot S)\,;F$.

Proof. See [Fri02], Thm 2.3. ∎

Filters are partial identities, i.e., relations F satisfying the condition $F \leq 1'$. Given a filter F, by $\neg F$ we denote the relation $\overline{F} \cdot 1'$.

Theorem A.2 *The following properties of filters are valid in all relation algebras:*

1. *If F is a filter, then $F + \neg F = 1'$*
2. *If F is a filter, then $F \cdot \neg F = 0$*
3. $\neg Dom(R) ; \mathbf{1} = \overline{R ; \mathbf{1}}$
4. *If F is functional, then*

$$F ; \neg Dom(R) ; \mathbf{1} = (Dom(F) \cdot \neg Dom(F ; R)) ; \mathbf{1}$$

5. *Let $F_1, \ldots, F_k$ be filters and let $i_1, \ldots, i_k$ be a permutation of $1, \ldots, k$, then*

$$F_1 ; \ldots ; F_k = F_{i_1} ; \ldots ; F_{i_k}$$

6. *If F is a filter, then $\neg F$ is a filter.*
7. *If F is a filter, then $F = F ; F$*
8. *If F is a filter, then $F ; R \leq R$ and $R ; F \leq R$*
9. *If F is a filter, then $R = (F ; R) + (\neg F ; R) = (R ; F) + (R ; \neg F)$*

Proof.

1. See [Fri02] Thm. 7.1.1.
2. See [Fri02] Thm. 7.1.2.
3. See [Fri02] Thm. 7.1.3.
4. See [Fri02] Thm. 7.1.4.
5.

$$\begin{aligned} F_1 ; \ldots ; F_k &= F_1 \cdot \ldots \cdot F_k && \text{(by Thm. A.1.7)} \\ &= F_{i_1} \cdot \ldots \cdot F_{i_k} && \text{(BA and Hyp)} \\ &= F_{i_1} ; \ldots ; F_{i_k} && \text{(by Thm. A.1.7)} \end{aligned}$$

6.

$$\begin{aligned} \neg F &= \overline{F} \cdot 1' && \text{(by def. } \neg\text{)} \\ &\leq 1' && \text{(by absorption)} \end{aligned}$$

7.

$$\begin{aligned} F &= F \cdot F && \text{(by idempotence)} \\ &= F;F && \text{(by Thm. A.1.7)} \end{aligned}$$

8.

$$\begin{aligned} F;R &\leq 1';R && \text{(by monotonicity and Hyp.)} \\ &= R && \text{(by Ax. 5)} \end{aligned}$$

The proof for $R;F \leq R$ follows in the same way.

9.

$$\begin{aligned} R &= 1';R && \text{(by Ax. 5)} \\ &= (F+\neg F);R && \text{(by 1)} \\ &= F;R+\neg F;R && \text{(by Ax. 2)} \end{aligned}$$

The proof for $R = F;R+\neg F;R$ follows in the same way.

■

Theorem A.3 *Let R be a right ideal relation, then the following properties are valid:*

1. *$\overline{R}$ is right ideal.*
2. *$Dom\left(\overline{R}\right) = \neg Dom\left(R\right)$*
3. *$Dom\left(R\right) \cdot Dom\left(\overline{R}\right) = 0$*
4. *$Dom\left(R\right) + Dom\left(\overline{R}\right) = 1'$*

Proof.

1. In order to prove this result we will use the following property of Boolean algebras. Let R and S be arbitrary, then

$$R \cdot S = 0 \Longrightarrow (R+S = \mathbf{1} \Longleftrightarrow S = \overline{R}) \qquad (7)$$

We have that,

$$\begin{aligned} \overline{R};\mathbf{1}+R &= \overline{R};\mathbf{1}+R;\mathbf{1} && \text{(by } R \text{ right ideal)} \\ &= (\overline{R}+R);\mathbf{1} && \text{(by Ax. 2)} \\ &= \mathbf{1};\mathbf{1} && \text{(BA)} \\ &= \mathbf{1} && \text{(by Thm. A.1.3)} \end{aligned}$$

Also,

$$
\begin{aligned}
\overline{R};\mathbf{1}\cdot R &= \overline{R};\mathbf{1}\cdot R;\mathbf{1} && \text{(by } R \text{ right ideal)}\\
&\geq (\overline{R}\cdot R);\mathbf{1} && \text{(by Thm. A.1.16)}\\
&= 0;\mathbf{1} && \text{(BA)}\\
&= 0 && \text{(by Thm. A.1.1)}
\end{aligned}
$$

Thus, by 7,

$$\overline{R};\mathbf{1} = \overline{R}$$

Therefore, $\overline{R}$ is right ideal.

2.

$$
\begin{aligned}
Dom\left(\overline{R}\right) &= Dom\left(\overline{R;\mathbf{1}}\right) && \text{(by } R \text{ right ideal)}\\
&= Dom\left(\neg Dom\left(R\right);\mathbf{1}\right) && \text{(by Thm. A.2.3)}\\
&= \left(\neg Dom\left(R\right);\mathbf{1};\mathbf{1}\right)\cdot 1\text{'} && \text{(by Thm. A.1.10)}\\
&= \left(\neg Dom\left(R\right);\mathbf{1}\right)\cdot 1\text{'} && \text{(by Thm. A.1.3)}\\
&= Dom\left(\neg Dom\left(R\right)\right) && \text{(by Thm. A.1.10)}\\
&= \neg Dom\left(R\right) && \text{(by Lemma A.1.1)}
\end{aligned}
$$

3.

$$
\begin{aligned}
Dom\left(R\right) + Dom\left(\overline{R}\right) &= Dom\left(R\right) + \neg Dom\left(R\right) && \text{(by 2)}\\
&= 1\text{'} && \text{(by Thm. A.2.1)}
\end{aligned}
$$

4.

$$
\begin{aligned}
Dom\left(R\right)\cdot Dom\left(\overline{R}\right) &= Dom\left(R\right)\cdot \neg Dom\left(R\right) && \text{(by 2)}\\
&= 0 && \text{(by Thm. A.2.2)}
\end{aligned}
$$

■

Lemma A.1 *The following properties are valid in all relation algebras:*

1. *If* $R \leq 1\text{'}$*, then* $Dom\left(R\right) = R$ *and* $Ran\left(R\right) = R$
2. *If* $R \leq 1\text{'}$*, then* $R\cdot 1\text{'} = R$
3. $Dom\left(R;S\right) = Dom\left(R;Dom\left(S\right)\right)$ *and* $Ran\left(R;S\right) = Ran\left(Ran\left(R\right);S\right)$
4. *If* $F \leq 1\text{'}$*, then* $Dom\left(F;R\right) = F;Dom\left(R\right)$ *and* $Ran\left(R;F\right) = Ran\left(R\right);F$
5. *If* F *functional, then* $Dom\left(F;S\right);F = F;Dom\left(S\right)$
6. *If* $R = R'$*,* $R\cdot T = 0$*,* $R'\cdot T' = 0$ *and* $R+T = R'+T'$*, then* $T = T'$

7. *If* $R \le S$, *then* $Ran(R) \le Ran(S)$ *and* $Dom(R) \le Dom(S)$

8. *If* $S \le 1'$, *then* $Ran(R) \le S \Longleftrightarrow R \le \mathbf{1};S$

9. *If* $R \le 1'$, *then* $R;S \le T \Longleftrightarrow S \le \neg R;\mathbf{1}+T$

10. *If* $R \le S$, *then* $R \cdot S = R$

11. *If* $Ran(R) \le Dom(S)$, *then* $R;S;\mathbf{1} = R;\mathbf{1}$

12. *If* Q *right ideal, then* $Dom\left(\overline{R;\overline{Q}}\right);R \le R;Dom(Q)$.

13. $R;(S+T) = (R;S)+(R;T)$.

14. $Dom(R) = Dom(R;\mathbf{1})$

Proof.

1.

$$\begin{aligned} Dom(R) &= R;\breve{R}\cdot 1' && \text{(def. } Dom\text{)} \\ &= R;R\cdot 1' && \text{(by Thm A.1.6)} \\ &= R\cdot R;1' && \text{(by Thm A.1.7)} \\ &= R\cdot R && \text{(by Ax. 5)} \\ &= R && \text{(BA)} \end{aligned}$$

The proof for *Ran* follows in a similar way.

2.

$$\begin{aligned} R\cdot 1' &= R;1' && \text{(by Thm A.1.7)} \\ &= R && \text{(by Ax. 5)} \end{aligned}$$

3.

$$\begin{aligned} Dom(R;S) &= (R;S;\mathbf{1})\cdot 1' && \text{(by Thm A.1.10)} \\ &= (R;Dom(S);\mathbf{1})\cdot 1' && \text{(by Thm A.1.14)} \\ &= Dom(R;Dom(S)) && \text{(by Thm A.1.10)} \end{aligned}$$

The proof for *Ran* is analogous to *Dom*.

4.

$$\begin{aligned} Dom(F;R) &= Dom(F;Dom(R)) && \text{(by 3)} \\ &= (F;Dom(R);(F;Dom(R))\breve{})\cdot 1' && \text{(by def. } Dom\text{)} \\ &= (F;Dom(R);(Dom(R))\breve{};\breve{F})\cdot 1' && \text{(by Ax. 6)} \\ &= (F\cdot Dom(R)\cdot \breve{F}\cdot (Dom(R))\breve{})\cdot 1' && \text{(by Thm A.1.7)} \\ &= (F\cdot Dom(R)\cdot F\cdot Dom(R))\cdot 1' && \text{(by Thm A.1.6)} \\ &= F\cdot Dom(R) && \text{(by 2 and BA)} \\ &= F;Dom(R) && \text{(by Thm. A.1.7)} \end{aligned}$$

The proof for *Ran* follows in a similar way.

5. In order to prove the equality we will prove both inclusions.

$\leq$)

$$\begin{aligned} F;Dom(S) &= Dom(F;Dom(S));F;Dom(S) && \text{(by Thm A.1.11)} \\ &= Dom(F;S);F;Dom(S) && \text{(by 3)} \\ &\leq Dom(F;S);F;1\text{'} && \text{(by def. } Dom\text{)} \\ &= Dom(F;S);F && \text{(by Ax. 5)} \end{aligned}$$

$\geq$)

$$\begin{aligned} Dom(F;S);F &= Dom(F;Dom(S));F && \text{(by 3)} \\ &= (((F;Dom(S));(F;Dom(S))^{\smile})\cdot 1\text{'});F && \text{(by def. } Dom\text{)} \\ &\leq F;Dom(S);(F;Dom(S))^{\smile};F && \text{(BA)} \\ &= F;Dom(S);(Dom(S))^{\smile};\breve{F};F && \text{(by Ax. 6)} \\ &\leq F;Dom(S);(Dom(S))^{\smile};1\text{'} && \text{(by } F \text{ functional)} \\ &= F;Dom(S);(Dom(S))^{\smile} && \text{(by Ax. 5)} \\ &= F;Dom(S);Dom(S) && \text{(by Thm A.1.6)} \\ &= F;Dom(S) && \text{(by Thm A.2.7)} \end{aligned}$$

6.

$$\begin{aligned} & R+T = R'+T' \\ \iff & R+T = R+T' && \text{(Hyp.)} \\ \implies & (R+T)\cdot\overline{R} = (R+T')\cdot\overline{R} && \text{(BA)} \\ \iff & R\cdot\overline{R}+T\cdot\overline{R} = R\cdot\overline{R}+T'\cdot\overline{R} && \text{(BA)} \\ \iff & T\cdot\overline{R} = T'\cdot\overline{R} && \text{(BA)} \\ \iff & T\cdot\overline{R} = T'\cdot\overline{R'} && \text{(Hyp.)} \end{aligned}$$

We have to show that $T\cdot\overline{R} = T$ and $T'\cdot\overline{R'} = T'$ to prove the lemma.

$$\begin{aligned} T &= T\cdot\mathbf{1} && \text{(BA)} \\ &= T\cdot(R+\overline{R}) && \text{(BA)} \\ &= T\cdot R+T\cdot\overline{R} && \text{(BA)} \\ &= T\cdot\overline{R} && \text{(Hyp.)} \end{aligned}$$

The proof for $T'\cdot\overline{R'} = T'$ follows in a similar way.

7.

$$\begin{aligned} Dom(R) &\leq Dom(R)+Dom(S) && \text{(BA)} \\ &= Dom(R+S) && \text{(by Thm A.1.12)} \\ &= Dom(S) && \text{(Hyp.)} \end{aligned}$$

The proof for *Ran* follows in a similar way.

8. $\Longrightarrow$)

$$
\begin{aligned}
R &= R;Ran\,(R) && \text{(by Thm A.1.11)}\\
&\leq R;S && \text{(by Hyp. and monotonicity)}\\
&\leq \mathbf{1};S && \text{(by monotonicity)}
\end{aligned}
$$

$\Longleftarrow$)

$$
\begin{aligned}
Ran\,(R) &\leq Ran\,(\mathbf{1};S) && \text{(by 7 and Hyp.)}\\
&= (\mathbf{1};(\mathbf{1};S))\cdot 1' && \text{(by def. } Ran\text{)}\\
&= (\mathbf{1};S)\cdot 1' && \text{(by Thm A.1.3)}\\
&= Ran\,(S) && \text{(by Thm A.1.10)}
\end{aligned}
$$

9. $\Longrightarrow$)

$$
\begin{aligned}
S &= 1';S && \text{(by Ax. 5)}\\
&= (R+\neg R);S && \text{(by Thm. A.2.1)}\\
&= R;S+\neg R;S && \text{(by Ax. 2)}\\
&\leq T+\neg R;S && \text{(Hyp.)}
\end{aligned}
$$

$\Longleftarrow$)

$$
\begin{aligned}
R;S &\leq R;(\neg R;\mathbf{1}+T) && \text{(Hyp.)}\\
&= R;\neg R;\mathbf{1}+R;T && \text{(by Ax. 2)}\\
&= (R\cdot\neg R);\mathbf{1}+R;T && \text{(by Thm A.1.7)}\\
&= (R\cdot\overline{R}\cdot 1');\mathbf{1}+R;T && \text{(by def. } \neg\text{)}\\
&= R;T && \text{(BA)}
\end{aligned}
$$

10. In order to prove the equality, we will prove both inclusions

$\geq$)

$$
\begin{aligned}
R\cdot S &= R\cdot(R+S) && \text{(Hyp.)}\\
&= R\cdot R+R\cdot S && \text{(BA)}\\
&= R+R\cdot S && \text{(by idempotence)}
\end{aligned}
$$

$\leq$)

$$
R+(R\cdot S) = R \qquad \text{(by absorption)}
$$

11.

$$
\begin{aligned}
R;S;\mathbf{1} &= R;Dom\,(S)\,;\mathbf{1} && \text{(by Thm A.1.14)}\\
&= R;Ran\,(R)\,;Dom\,(S)\,;\mathbf{1} && \text{(by Thm A.1.11)}\\
&= R;(Ran\,(R)\cdot Dom\,(S));\mathbf{1} && \text{(by Thm A.1.7)}\\
&= R;Ran\,(R)\,;\mathbf{1} && \text{(by Hyp. and 10)}\\
&= R;\mathbf{1} && \text{(by Thm A.1.11)}
\end{aligned}
$$

12.

$$
\begin{aligned}
& Dom\left(\overline{R;\overline{Q}}\right);R \\
&= \neg Dom\left(R;\overline{Q}\right);R && \text{(by Thm. A.3.2)} \\
&= \neg Dom\left(R;Dom\left(\overline{Q}\right)\right);R && \text{(by Lemma A.1.3)} \\
&= \neg Dom\left(R;\neg Dom\left(Q\right)\right);R && \text{(by Thm. A.3.2)} \\
&= \neg Dom\left(R;\neg Dom\left(Q\right)\right);R;Dom\left(Q\right) \\
&\qquad + \neg Dom\left(R;\neg Dom\left(Q\right)\right);R;\neg Dom\left(Q\right)) && \text{(by Thm. A.2.9)} \\
&= \neg Dom\left(R;\neg Dom\left(Q\right)\right);R;Dom\left(Q\right) \\
&\qquad + \neg Dom\left(R;\neg Dom\left(Q\right)\right);Dom\left(R;\neg Dom\left(Q\right)\right);R;\neg Dom\left(Q\right)) \\
& && \text{(by Thm A.1.11)} \\
&= \neg Dom\left(R;\neg Dom\left(Q\right)\right);R;Dom\left(Q\right) \\
&\qquad + \left(\neg Dom\left(R;\neg Dom\left(Q\right)\right)\cdot Dom\left(R;\neg Dom\left(Q\right)\right)\right);R;\neg Dom\left(Q\right)) \\
& && \text{(by Thm A.1.7)} \\
&= \neg Dom\left(R;\neg Dom\left(Q\right)\right);R;Dom\left(Q\right) && \text{(by Thm. A.2.2)} \\
&\leq R;Dom\left(Q\right) && \text{(by Thm. A.2.8)}
\end{aligned}
$$

13.

$$
\begin{aligned}
R;(S+T) &= ((R;(S+T))^{\smile})^{\smile} && \text{(by Ax. 4)} \\
&= \left((S+T)^{\smile};\breve{R}\right)^{\smile} && \text{(by Ax. 6)} \\
&= \left((\breve{S}+\breve{T});\breve{R}\right)^{\smile} && \text{(by Ax. 3)} \\
&= \left(\breve{S};\breve{R}+\breve{T};\breve{R}\right)^{\smile} && \text{(by Ax. 2)} \\
&= ((R;S)^{\smile}+(R;T)^{\smile})^{\smile} && \text{(by Ax. 6)} \\
&= (((R;S)+(R;T))^{\smile})^{\smile} && \text{(by Ax. 3)} \\
&= (R;S)+(R;T) && \text{(by Ax. 4)}
\end{aligned}
$$

14.

$$
\begin{aligned}
Dom\left(R\right) &= (R;\mathbf{1})\cdot 1' && \text{(by Thm. A.1.10)} \\
&= (R;\mathbf{1};\mathbf{1})\cdot 1' && \text{(by } R;\mathbf{1} \text{ right ideal)} \\
&= Dom\left(R;\mathbf{1}\right) && \text{(by Thm. A.1.10)}
\end{aligned}
$$

■

Theorem A.4 *The following properties hold in all fork algebras for all relations F, I, R, S, T and U.*

1. $(R\nabla S);\breve{2} = R\cdot S$.

2. $(R \nabla S)\,;\pi = Dom\,(S)\,;R$ *and* $(R \nabla S)\,;\rho = Dom\,(R)\,;S$.

3. $R;\,(S \nabla T) \leq (R;S) \nabla (R;T)$.

4. *Let* F *be functional, then* $F;\,(R \nabla S) = (F;R) \nabla (F;S)$.

5. *If* $F \leq 1'$ *then* $(F;R) \nabla S = F;\,(R \nabla S)$.

6. $(R \nabla S) \cdot (T \nabla U) = (R \cdot T) \nabla (S \cdot U)$.

7. $(R \otimes S)^{\smile} = \breve{R} \otimes \breve{S}$.

8. $(R \otimes S) \cdot (T \otimes U) = (R \cdot T) \otimes (S \cdot U)$.

9. $(R \nabla S)\,;(T \otimes U) = (R;T) \nabla (S;U)$.

10. $(R \otimes S)\,;(T \otimes U) = (R;T) \otimes (S;U)$.

11. $(R+S) \otimes T = (R \otimes T) + (S \otimes T)$, *i.e.,* $\otimes$ *is additive. Similarly,* $R \otimes (S+T) = (R \otimes S) + (R \otimes T)$.

12. $(R \otimes 1')\,;\pi = \pi;R$ *and* $(1' \otimes R)\,;\rho = \rho;R$.

13. *The relations* π *and* ρ *are functional.*

14. $\breve{\pi};\rho = \mathbf{1}$.

15. $Dom\,(\pi) = Dom\,(\rho) = 1' \otimes 1'$.

16. $Dom\,(\pi;R) = Dom\,(R) \otimes 1'$ *and* $Dom\,(\rho;R) = 1' \otimes Dom\,(R)$.

17. $(\breve{R} \otimes 1');\breve{2} = Dom\,((1' \otimes R)\,;\breve{2})\,;\rho$.

18. *Let* F *be functional, then* $\breve{\pi} \cdot \mathbf{1};(1' \nabla F) = 1' \nabla F$.

19. *If* I *is injective, then* $(1' \otimes R;I)\,;\breve{2} = Dom\left((\breve{I} \otimes R);\breve{2}\right);\pi$ *and* $(R;I \otimes 1')\,;\breve{2} = Dom\left((R \otimes \breve{I});\breve{2}\right);\rho$.

20. $(1' \otimes 1')\,;\overline{R \otimes S};\,(1' \otimes 1') = (\overline{R} \otimes \mathbf{1}) + (\mathbf{1} \otimes \overline{S})$.

Proof. See [Fri02] Thm. 3.2.. ■

Lemma A.2 *The following properties are valid in all abstract fork algebras for all relations* R, S, T *and* U.

1. *If* $R \leq S$ *and* $T \leq U$, *then* $R \nabla T \leq S \nabla U$ *and* $R \otimes T \leq S \otimes U$.

2. $Dom\,(R \nabla S) = Dom\,(R) \cdot Dom\,(S)$

3. $\pi;\breve{\pi} = 1' \otimes \mathbf{1}$

4. $\rho;R;\breve{\rho} = \mathbf{1} \otimes R$

5. *If $R,T \leq 1'$, then*

$$Ran\left(\begin{pmatrix}\pi\\ \nabla\\ \begin{pmatrix}R;S;T\\ \otimes\\ \rho\end{pmatrix}\end{pmatrix}\right);\rho = Ran\left(\begin{pmatrix}\pi\\ \nabla\\ \begin{pmatrix}R;S;T\\ \otimes\\ \rho\end{pmatrix}\end{pmatrix}\right);\begin{pmatrix}R\\ \otimes\\ 1'\end{pmatrix};\rho;\begin{pmatrix}T\\ \otimes\\ 1'\end{pmatrix}$$

Proof.

1. We will prove the first property, namely, that

$$R\nabla T \leq S\nabla U \tag{8}$$

We proceed as follows.

$$\begin{aligned} R\nabla T &= R;\breve{\pi}\cdot T;\breve{\rho} && \text{(by Ax. 8)}\\ &\leq S;\breve{\pi}\cdot U;\breve{\rho} && \text{(by monotonicity)}\\ &= S\nabla U && \text{(by Ax. 8)}\end{aligned}$$

We will finally show that $R\otimes T \leq S\otimes U$

$$\begin{aligned} R\otimes T &= \pi;R\nabla\rho;T && \text{(by def. }\otimes)\\ &\leq \pi;S\nabla\rho;U && \text{(by (8) and monotonicity of ;)}\\ &= S\otimes U && \text{(by def. }\otimes)\end{aligned}$$

2. First note that

$$Ran\,(\mathbf{1}\nabla\mathbf{1}) = 1'\otimes 1' \tag{9}$$

Then,

$$\begin{aligned} Dom\,(R\nabla S) &= Dom\,(R;1'\nabla S;1') && \text{(by Ax. 5)}\\ &= Dom\,((R\nabla S);(1'\otimes 1')) && \text{(by Thm. A.4.9)}\\ &= Dom\,(R\nabla S;Ran\,(\mathbf{1}\nabla\mathbf{1})) && \text{(by (9))}\\ &= Dom\,(R\nabla S;Dom\,((\mathbf{1}\nabla\mathbf{1})^{\smile})) && \text{(by Thm. A.1.13)}\\ &= Dom\,(R\nabla S;(\mathbf{1}\nabla\mathbf{1})^{\smile}) && \text{(by Lemma A.1.3)}\\ &= Dom\,((R;\breve{\mathbf{1}})\cdot(S;\breve{\mathbf{1}})) && \text{(by Ax. 9)}\\ &= Dom\,((R;\mathbf{1})\cdot(S;\mathbf{1})) && \text{(by Thm. A.1.2)}\\ &= (((R;\mathbf{1})\cdot(S;\mathbf{1}));\mathbf{1})\cdot 1' && \text{(by Thm. A.1.10)}\\ &= (R;\mathbf{1})\cdot(S;\mathbf{1})\cdot 1' && \text{(because }(R;\mathbf{1})\cdot(S;\mathbf{1})\text{ is right ideal)}\\ &= (R;\mathbf{1})\cdot 1'\cdot(S;\mathbf{1})\cdot 1' && \text{(by idempotence)}\\ &= Dom\,(R)\cdot Dom\,(S) && \text{(by Thm. A.1.10)}\end{aligned}$$

3. In order to prove the property, we will show that

$$\rho;\mathbf{1};\breve{\rho} = \pi;\mathbf{1};\breve{\pi} \tag{10}$$

$$
\begin{aligned}
\rho;\mathbf{1};\breve{\rho} &= Dom\,(\rho)\,;\mathbf{1};Ran\,(\breve{\rho}) && \text{(by Thm. A.1.14)}\\
&= Dom\,(\rho)\,;\mathbf{1};Dom\,(\rho) && \text{(by Thm. A.1.13)}\\
&= Dom\,(\pi)\,;\mathbf{1};Dom\,(\pi) && \text{(by Thm. A.4.15)}\\
&= Dom\,(\pi)\,;\mathbf{1};Ran\,(\breve{\pi}) && \text{(by Thm. A.1.13)}\\
&= \pi\,;\mathbf{1};\breve{\pi} && \text{(by Thm. A.1.14)}
\end{aligned}
$$

Second, we prove that

$$
\begin{aligned}
\pi\,;\breve{\pi} &= \pi\,;1'\,;\breve{\pi} && \text{(by Ax. 5)}\\
&\leq \pi\,;\mathbf{1};\breve{\pi} && \text{(by monotonicity)}
\end{aligned}
$$

Then,

$$
\pi\,;\breve{\pi} \leq \pi\,;\mathbf{1};\breve{\pi} \tag{11}
$$

Once both results were established, we proceed as follows.

$$
\begin{aligned}
\pi\,;\breve{\pi} &= (\pi\,;\breve{\pi})\cdot(\pi\,;\mathbf{1};\breve{\pi}) && \text{(by (11))}\\
&= (\pi\,;\breve{\pi})\cdot(\rho;\mathbf{1};\breve{\rho}) && \text{(by (10))}\\
&= (\pi\,;1'\,;\breve{\pi})\cdot(\rho;\mathbf{1};\breve{\rho}) && \text{(by Ax. 5)}\\
&= \pi\,;1'\,\nabla\,\rho;\mathbf{1} && \text{(by Ax. 8)}\\
&= 1'\otimes\mathbf{1} && \text{(by def. }\otimes)
\end{aligned}
$$

4. The proof begins by showing that

$$
\rho;R;\breve{\rho} \leq \pi\,;\mathbf{1};\breve{\pi} \tag{12}
$$

$$
\begin{aligned}
\rho;R;\breve{\rho} &\leq \rho;\mathbf{1};\breve{\rho} && \text{(by monotonicity)}\\
&= \pi\,;\mathbf{1};\breve{\pi} && \text{(by (10))}
\end{aligned}
$$

Finally, we proceed as follows,

$$
\begin{aligned}
\rho;R;\breve{\rho} &= (\rho;R;\breve{\rho})\cdot(\pi\,;\mathbf{1};\breve{\pi}) && \text{(by (12))}\\
&= \pi\,;\mathbf{1}\nabla\rho;R && \text{(by Ax. 8)}\\
&= \mathbf{1}\otimes R && \text{(by def. }\otimes)
\end{aligned}
$$

5. First, we have that, if $R, T \leq 1'$, then

$$
(R\otimes(T\otimes 1'));\rho = (R\otimes 1');\rho;(T\otimes 1') \tag{13}
$$

$$
\begin{aligned}
(R\otimes(T\otimes 1'));\rho &= (\pi\,;R\nabla\rho;(T\otimes 1'));\rho && \text{(by def. }\otimes)\\
&= Dom\,(\pi\,;R)\,;\rho;(T\otimes 1') && \text{(by Thm. A.4.2)}\\
&= (Dom\,(R)\otimes 1');\rho;(T\otimes 1') && \text{(by Thm. A.4.16)}\\
&= (R\otimes 1');\rho;(T\otimes 1') && \text{(by Lemma A.1.1)}
\end{aligned}
$$

We also have that, if $R, T \leq 1'$, then

$$\left(\begin{array}{c}\pi\\ \nabla\\ \left(\begin{array}{c}R;S;T\\ \otimes\\ \rho\end{array}\right)\end{array}\right) = \left(\begin{array}{c}\pi\\ \nabla\\ \left(\begin{array}{c}\pi;R;S;T\\ \nabla\\ \rho;\rho\end{array}\right)\end{array}\right) \qquad \text{(by def. } \otimes)$$

$$= \left(\begin{array}{c}\pi\\ \nabla\\ (\pi;R)\nabla(\rho;1');((S;T)\otimes\rho)\end{array}\right) \qquad \text{(by Thm. A.4.9)}$$

$$= \left(\begin{array}{c}\pi\\ \nabla\\ (R\otimes 1');((S;T)\otimes\rho)\end{array}\right) \qquad \text{(by def. } \otimes)$$

$$= \left(\begin{array}{c}(R\otimes 1');\pi\\ \nabla\\ (S;T)\otimes\rho\end{array}\right) \qquad \text{(by Thm. A.4.5)}$$

$$= \left(\begin{array}{c}\pi;R\\ \nabla\\ (S;T)\otimes\rho\end{array}\right) \qquad \text{(by Thm. A.4.12)}$$

$$= \left(\begin{array}{c}\pi;R\\ \nabla\\ (S;T)\otimes(\rho;1')\end{array}\right) \qquad \text{(by Ax. 5)}$$

$$= \left(\begin{array}{c}\pi;R\\ \nabla\\ (S\otimes\rho);(T\otimes 1')\end{array}\right) \qquad \text{(by Thm. A.4.10)}$$

$$= \left(\begin{array}{c}\pi\\ \nabla\\ (S\otimes\rho)\end{array}\right);\left(\begin{array}{c}R\\ \otimes\\ (T\otimes 1')\end{array}\right) \qquad \text{(by Thm. A.4.9)}$$

Since,

$$Ran\left(\begin{array}{c}\pi\\ \nabla\\ \left(\begin{array}{c}R;S;T\\ \otimes\\ \rho\end{array}\right)\end{array}\right) = Ran\left(\left(\begin{array}{c}\pi\\ \nabla\\ (S\otimes\rho)\end{array}\right);\left(\begin{array}{c}R\\ \otimes\\ (T\otimes 1')\end{array}\right)\right)$$

$$= Ran\left(\left(\begin{array}{c}\pi\\ \nabla\\ (S\otimes\rho)\end{array}\right)\right);\left(\begin{array}{c}R\\ \otimes\\ (T\otimes 1')\end{array}\right) \qquad \text{(by Lemma A.1.4)}$$

$$\leq \left(\begin{array}{c}R\\ \otimes\\ (T\otimes 1')\end{array}\right) \qquad \text{(by Thm. A.2.8)}$$

Therefore, we have

$$Ran\left(\begin{array}{c}\pi\\ \nabla\\ \left(\begin{array}{c}R;S;T\\ \otimes\\ \rho\end{array}\right)\end{array}\right) \leq \left(\begin{array}{c}R\\ \otimes\\ (T\otimes 1')\end{array}\right) \tag{14}$$

Finally, we prove the lemma by showing both inclusions

$\leq$)

$$\begin{aligned}
& Ran\left(\begin{array}{c}\pi\\ \nabla\\ \left(\begin{array}{c}R;S;T\\ \otimes\\ \rho\end{array}\right)\end{array}\right);\rho \\
= \; & Ran\left(\begin{array}{c}\pi\\ \nabla\\ \left(\begin{array}{c}R;S;T\\ \otimes\\ \rho\end{array}\right)\end{array}\right);Ran\left(\begin{array}{c}\pi\\ \nabla\\ \left(\begin{array}{c}R;S;T\\ \otimes\\ \rho\end{array}\right)\end{array}\right);\rho \\
& \qquad \text{(by Thm. A.2.7)} \\
\leq \; & Ran\left(\begin{array}{c}\pi\\ \nabla\\ \left(\begin{array}{c}R;S;T\\ \otimes\\ \rho\end{array}\right)\end{array}\right);\left(\begin{array}{c}R\\ \otimes\\ \left(\begin{array}{c}T\\ \otimes\\ 1'\end{array}\right)\end{array}\right);\rho \qquad \text{(by (14))} \\
= \; & Ran\left(\begin{array}{c}\pi\\ \nabla\\ \left(\begin{array}{c}R;S;T\\ \otimes\\ \rho\end{array}\right)\end{array}\right);\left(\begin{array}{c}R\\ \otimes\\ 1'\end{array}\right);\rho;\left(\begin{array}{c}T\\ \otimes\\ 1'\end{array}\right) \qquad \text{(by (13))}
\end{aligned}$$

$\geq$)

$$\begin{aligned}
& Ran\left(\begin{array}{c}\pi\\ \nabla\\ \left(\begin{array}{c}R;S;T\\ \otimes\\ \rho\end{array}\right)\end{array}\right);\left(\begin{array}{c}R\\ \otimes\\ 1'\end{array}\right);\rho;\left(\begin{array}{c}T\\ \otimes\\ 1'\end{array}\right) \\
\leq \; & Ran\left(\begin{array}{c}\pi\\ \nabla\\ \left(\begin{array}{c}R;S;T\\ \otimes\\ \rho\end{array}\right)\end{array}\right);\rho \qquad \text{(by Thm. A.2.8)}
\end{aligned}$$

■

Lemma A.3 *If $F \leq 1'$ and $Ran\,(F;R) \leq F$, then,*

$$F;R^* = F;(F;R;F)^* = F;R^*;F$$

Proof. In order to prove this property, we will show that, if $Ran\,(F;R) \leq F$ and F is a filter, then,

$$R^* = F;(F;R)^*;F + \neg F;R^* \tag{15}$$

$\geq$)

$$\begin{aligned} R^* &= 1';R^* && \text{(by Ax. 5)} \\ &= (F+\neg F);R^* && \text{(by Thm.A.2.1)} \\ &= F;R^* + \neg F;R^* && \text{(by Thm.A.1.13)} \\ &\geq F;(F;R)^*;F + \neg F;R^* && \text{(by monotonicity)} \end{aligned}$$

$\leq$) We prove this inclusion by using the ω-rule.

- base case.

$$\begin{aligned} & 1' + F;(F;R)^*;F + \neg F;R^* \\ &= 1' + F;(1' + (F;R);(F;R)^*);F + \neg F;(1' + R;R^*) && \text{(by Ax. 14)} \\ &= 1' + (F;1' + F;F;R;(F;R)^*);F + \neg F;1' + \neg F;R;R^* \\ & && \text{(by Thm.A.1.13)} \\ &= 1' + F;1';F + F;F;R;(F;R)^*;F + \neg F;1' + \neg F;R;R^* && \text{(by Ax. 2)} \\ &= 1' + (F + \neg F) + F;R;(F;R)^* + \neg F;R;R^* \\ & && \text{(by Ax. 5 and Thm. A.2.7)} \\ &= (F + \neg F) + F;R;(F;R)^* + \neg F;R;R^* && \text{(by Thm.A.2.1)} \\ &= F;(F;R)^* + \neg F;R^* && \text{(by Axs. 2, 5 and 14, and Lemma A.1.13)} \end{aligned}$$

Therefore,

$$1' \leq F;(F;R)^*;F + \neg F;R^*$$

- inductive step.

$$
\begin{aligned}
R^{i+1} &= R;R^i && \text{(by def. 2.33)}\\
&\leq R;(F;(F;R)^*;F+\neg F;R^*) && \text{(by Ind. Hyp.)}\\
&= R;F;(F;R)^*;F+R;\neg F;R^* && \text{(by Lemma A.1.13)}\\
&= F;R;F;(F;R)^*;F+\neg F;R;F;(F;R)^*;F\\
&\quad +F;R;\neg F;R^*+\neg F;R;\neg F;R^* && \text{(by Thm. A.2.9)}\\
&= F;R;F;(F;R)^*;F+\neg F;R;F;(F;R)^*;F\\
&\quad +F;R;F;\neg F;R^*+\neg F;R;\neg F;R^* && \text{(by Hyp.)}\\
&= F;R;F;(F;R)^*;F+\neg F;R;F;(F;R)^*;F\\
&\quad +F;R;(F\cdot\neg F);R^*+\neg F;R;\neg F;R^* && \text{(by Thm. A.1.7)}\\
&= F;R;F;(F;R)^*;F+\neg F;R;F;(F;R)^*;F\\
&\quad +\neg F;R;\neg F;R^* && \text{(by Thm. A.2.2)}\\
&\leq F;R;F;(F;R)^*;F+\neg F;R;R^*\\
&\quad +\neg F;R;R^* && \text{(by Thm. A.2.8)}\\
&= F;R;F;(F;R)^*;F\\
&\quad +\neg F;R;R^* && \text{(by idempotence)}\\
&= F;F;R;F;(F;R)^*;F\\
&\quad +\neg F;R;R^* && \text{(by Thm A.2.7)}\\
&\leq F;F;R;(F;R)^*;F\\
&\quad +\neg F;R;R^* && \text{(by Thm A.2.8)}\\
&\leq F;(F;R)^*;F+\neg F;R^* && \text{(by Ax. 14)}
\end{aligned}
$$

Now we will show that the lemma is valid.

- $F;R^* = F;(F;R;F)^*$

$\leq$)

$$
\begin{aligned}
F;R^* &= F;(F;(F;R)^*;F+\neg F;R^*) && \text{(by (15))}\\
&= F;F;(F;R)^*;F+F;\neg F;R^* && \text{(by Lemma A.1.13)}\\
&= F;(F;R)^*;F+F;\neg F;R^* && \text{(by Thm. A.2.7)}\\
&= F;(F;R)^*;F+(F\cdot\neg F);R^* && \text{(by Thm. A.1.7)}\\
&= F;(F;R)^*;F && \text{(by Thm. A.2.2)}\\
&= F;(F;R;F)^*;F && \text{(by Hyp.)}\\
&\leq F;(F;R;F)^* && \text{(by monotonicity)}
\end{aligned}
$$

$\geq$)

$$
F;R^* \geq F;(F;R;F)^* \qquad \text{(by monotonicity)}
$$

- $F;R^* = F;R^*;F$

$\leq$)

$$\begin{aligned}
F;R^* &= F;(F;(F;R)^*;F+\neg F;R^*) && \text{(by (15))} \\
&= F;F;(F;R)^*;F+F;\neg F;R^* && \text{(by Lemma A.1.13)} \\
&\leq F;R^*;F+F;\neg F;R^* && \text{(by monotonicity)} \\
&= F;R^*;F+(F\cdot\neg F);R^* && \text{(by Thm. A.1.7)} \\
&= F;R^*;F && \text{(by Thm. A.2.2)}
\end{aligned}$$

$\geq$)

$$F;R^* \geq F;R^*;F \qquad \text{(by monotonicity)}$$

■

B On DLTL interpretation

Lemma B.1 *Let K be a Kripke structure. Let $s \in \Delta_K$ and $n \in \mathbb{N}$.*

$$exec(s,n) \in \|P\|_K;\|Q\|_K$$
$$\iff$$
$$(\exists i \in [0,n])(exec(s,i) \in \|P\|_K \wedge exec(s^i, n-i) \in \|Q\|_K)$$

Proof.

$$exec(s,n) \in \|P\|_K;\|Q\|_K$$
$$\iff$$
$$\begin{array}{l}(\exists \tau)(\exists \tau')(\\ (exec(s,n) = \tau;\tau')\wedge\\ (\tau \in \|P\|_K \wedge \tau' \in \|Q\|_K)\wedge\\ (\tau = \lambda \vee \tau' = \lambda \vee \tau_{|\tau|-1} = \tau'_0))\end{array}$$

$\iff$ by def. 5.3

$$\begin{array}{l}(\exists \tau)(\exists \tau')(\\ (exec(s,n) = \tau;\tau')\wedge\\ (\tau \in \|P\|_K \wedge \tau' \in \|Q\|_K)\wedge\\ ((exec(s,n) = \tau') \vee (exec(s,n) = \tau) \vee (exec(s,n) = \tau\&\tau'^1)))\end{array}$$

$\iff$ by def. 5.7

$$\begin{array}{l}(\exists \tau)(\exists \tau')(\\ (exec(s,n) = \tau;\tau')\wedge\\ (\tau \in \|P\|_K \wedge \tau' \in \|Q\|_K)\wedge\\ ((exec(s,n) = \tau') \vee (exec(s,n) = \tau)\vee\\ (\exists i \in (0,n))(exec(s,i) = \tau \wedge exec(s^i, n-i) = \tau')))\end{array}$$
$$\iff$$
$$\begin{array}{l}(exec(s,n) \in \|P\|_K \wedge \lambda \in \|Q\|_K)\vee\\ (\lambda \in \|P\|_K \wedge exec(s,n) \in \|Q\|_K)\vee\\ (\exists i \in (0,n))(exec(s,i) \in \|P\|_K \wedge exec(s^i, n-i) \in \|Q\|_K)\end{array}$$

$\iff$ by def. 5.7

$$\begin{array}{l}(exec(s,n) \in \|P\|_K \wedge exec(s^n, n-n) \in \|Q\|_K)\vee\\ (exec(s,0) \in \|P\|_K \wedge exec(s^0, n-0) \in \|Q\|_K)\vee\\ (\exists i \in (0,n))(exec(s,i) \in \|P\|_K \wedge exec(s^i, n-i) \in \|Q\|_K)\end{array}$$
$$\iff$$
$$(\exists i \in [0,n])(exec(s,i) \in \|P\|_K \wedge exec(s^i, n-i) \in \|Q\|_K)$$

■

We present all the necessary definitions to end with the main result on the interpretability of $DLTL$. Most of them were also presented in [FP03] to prove the interpretability of LTL.

Lemma B.2 *Given a nonempty set S, a binary relation T (on S), and a sequence of T-connected elements of S, namely, $s = s_0, s_1, s_2, \ldots$,*

$$(\forall i < \omega)(t_{s^i} = \rho^i(t_s))$$

Proof. The proof follows by an easy induction on i. ■

Lemma B.3 *Given a nonempty set S, a binary relation T (on S), and $t \in \mathcal{T}(S,T)$, $(\forall i < \omega)(s_{\rho^i(t)} = (s_t)^i)$.*

Proof. The proof follows by a simple induction on i. ■

Definition B.1 ([FP03]) *Let S be a nonempty set, and T a binary relation on S. We denote by $\mathcal{T}(S,T)^\star$ the smallest set R of binary trees built as follows:*

- *$S \cup \mathcal{T}(S,T) \subseteq R$,*
- *if $t_1, t_2 \in R$, then $t_1 \star t_2 \in R$.*

Definition B.2 *Let S be a nonempty set, and $\tilde{A} = \{\tilde{a_i}\}_{i \in \mathcal{A}}$ a set of binary relations on S. We define,*

$$T_{\tilde{A}} = \bigcup_{i \in \mathcal{A}} \tilde{a_i}$$

When no confusion arise, we will simply denote $T_{\tilde{A}}$ as T.

Definition B.3 ([FP03]) *Let S be a nonempty set, and $\tilde{A} = \{\tilde{a_i}\}_{i \in \mathcal{A}}$ a set of binary relations on S. Let $\mathfrak{A} = \langle R, \cup, \cap, ^-, \emptyset, E, \circ, Id, ^\smile, \underline{\nabla}, ^\diamond, ^* \rangle$ be a proper closure fork algebra* (PCFA) *satisfying:*

- *$R = \mathcal{P}(\mathcal{T}(S,T)^\star \times \mathcal{T}(S,T)^\star)$,*
- *$E = \mathcal{T}(S,T)^\star \times \mathcal{T}(S,T)^\star$*

$\mathfrak{A}$ is then called a "full infinite closure fork algebra on $S, \tilde{A}$".

Definition B.4 ([FP03]) *Given $\mathfrak{A} = \langle R, \cup, \cap, ^-, \emptyset, E, \circ, Id, ^\smile, \underline{\nabla}, ^\diamond, ^* \rangle \in$ PCFA, we define:*

- *$\pi(x \star y) = x$ for all $x, y \in U_{\mathfrak{A}}$,*
- *$\rho(x \star y) = y$ for all $x, y \in U_{\mathfrak{A}}$.*

Notice that no confusion should arise between the relation constants π and ρ and the functions π and ρ from Def. B.4; while the former are relational constants, the latter are functions and always appear being applied to arguments.

Definition B.5 ([FP03]) *Given $K = \langle S, \tilde{A}, S_0, \tilde{P} \rangle$ a Kripke structure for the signature Σ and let $\langle R, +, \cdot, ^-, 0, \mathbf{1}, ;, \mathbf{1}', ^\smile, \nabla, ^\diamond, ^* \rangle$ be a full infinite closure fork algebra on S and $\tilde{A}$, extended with constants $\mathbf{S}$, $\mathbf{S_0}$, $\mathbf{T}$, $\mathbf{tr}$, $\{\mathbf{P_i}\}_{i \in \mathcal{P}}$, $\{\mathbf{A_i}\}_{i \in \mathcal{A}}$, satisfying:*

- $\mathbf{S} = \{\langle s, s\rangle \,|s \in S\}$,

- $\mathbf{S_0} \subseteq \mathbf{S}$,

- $\mathbf{T} = T$,

- $\mathbf{tr} = \{\langle t, t\rangle \,|t \in \mathcal{T}(S, T)\}$,

- $\mathsf{dom}\,(\mathbf{P_i}) \subseteq \mathbf{S}$ *and* $\mathbf{P_i}$ *is right-ideal for all* $i \in \mathcal{P}$, *and*

- $\mathbf{A_i} = \tilde{a}_i$ *for all* $i \in \mathcal{A}$;

we call $\mathfrak{A}$ *a "full infinite closure fork algebra on* S,$\tilde{A}$ *extended with constants"*

It follows from the previous definition that every full infinite closure fork algebra on S, $\tilde{A}$, extended with constants satisfies the axioms of ω-CCFA^{+DLTL}.

Lemma B.4 *Let* $K = \langle S, \tilde{A}, S_0, \tilde{P}\rangle$ *be a Kripke structure for the signature* Σ, *and let* $\mathfrak{A}$ *a full infinite closure fork algebra on* S, $\tilde{A}$, *extended with constants. Then,*

$$s \in \Delta_K \Longleftrightarrow t_s \in \mathsf{dom}\,(\mathbf{tr}) \ .$$

Proof.

$\Rightarrow$) Since $s \in \Delta_K$, s is a T-connected sequence of elements of S. Then, by Def. 4.6, $t_s \in \mathcal{T}(S, T)$. Thus, by definition of $\mathbf{S}$, $\mathbf{T}$ and $\mathbf{tr}$, $t_s \in \mathsf{dom}\,(\mathbf{tr})$.

$\Leftarrow$) Assume that $t_s \in \mathsf{dom}\,(\mathbf{tr})$. By definition of $\mathbf{S}$, $\mathbf{T}$ and $\mathbf{tr}$, $t_s \in \mathcal{T}(S, T)$, and by Def. 4.6, s is a T-connected sequence of elements of S. Then, by definition of trace in a Kripke structure, $s \in \Delta_K$.

∎

Lemma B.5 *Let* $K = \langle S, \tilde{A}, S_0, \tilde{P}\rangle$ *be a Kripke structure for the signature* Σ, *and let* $\mathfrak{A}$ *be a full infinite closure fork algebra on* S *and* $\tilde{A}$, *extended with constants.. Then,*

$$t \in \mathsf{dom}\,(\mathbf{tr}) \Longleftrightarrow s_t \in \Delta_K \ .$$

Proof.

$\Rightarrow$) Since $t \in \mathsf{dom}\,(\mathbf{tr})$, $t \in \mathcal{T}(S, T)$. Since consecutive elements in t are T-connected, s_t is a T-connected sequence of elements of S. Finally, by definition of K, $s_t \in \Delta_K$.

$\Leftarrow$) Assume that $s_t \in \Delta_K$. Since s_t is a T-connected sequence of elements of S, $t \in \mathcal{T}(S, T) = \mathsf{dom}\,(\mathbf{tr})$.

∎

Lemma B.6 *Let $K = \langle S, \tilde{A}, S_0, \tilde{P} \rangle$ be a Kripke structure for the signature Σ, and let $\mathfrak{A}$ be a full infinite closure fork algebra on S and $\tilde{A}$, extended with constants. If $\alpha \in ForDLTL(\Sigma)$, and $t, t' \in \mathcal{T}(S,T)$, then*

$$
\begin{array}{l}
(\exists i \geq 0)(\exists i' \geq 0)(\exists t'')(\\
\quad (t'' = \rho^i(t)) \wedge (\forall j \in [0,i))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)))\wedge \\
\quad (exec(s_t, i) \in \|P\|_K) \wedge \\
\quad (t' = \rho^{i'}(t'')) \wedge (\forall j \in [0,i'))(\rho^j(t'') \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)))\wedge \\
\quad (exec(s_{t''}, i') \in \|Q\|_K))
\end{array}
$$

$\iff$

$$
\begin{array}{l}
(\exists n \geq 0)(\\
\quad (t' = \rho^n(t)) \wedge (\forall j \in [0,n))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)))\wedge \\
\quad (exec(s_t, n) \in \|P\|_K ; \|Q\|_K))
\end{array}
$$

Proof.

$$
\begin{array}{l}
(\exists i \geq 0)(\exists i' \geq 0)(\exists t'')(\\
\quad t'' = \rho^i(t) \wedge (\forall j \in [0,i))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)))\wedge \\
\quad exec(s_t, i) \in \|P\|_K \wedge \\
\quad t' = \rho^{i'}(t'') \wedge (\forall j \in [0,i'))(\rho^j(t'') \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)))\wedge \\
\quad exec(s_{t''}, i') \in \|Q\|_K)
\end{array}
$$

$\iff$ because $t'' = \rho^i(t)$

$$
\begin{array}{l}
(\exists i \geq 0)(\exists i' \geq 0)(\\
\quad (\forall j \in [0,i))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)))\wedge \\
\quad exec(s_t, i) \in \|P\|_K \wedge \\
\quad t' = \rho^{i'}(\rho^i(t)) \wedge (\forall j \in [0,i'))(\rho^j(\rho^i(t)) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)))\wedge \\
\quad exec(s_{\rho^i(t)}, i') \in \|Q\|_K)
\end{array}
$$

$\iff$

$$
\begin{aligned}
&(\exists i \geq 0)(\exists i' \geq 0)(\\
&\quad t' = \rho^{i'}(\rho^{i}(t)) \wedge \\
&\quad (\forall j \in [0,i))(\rho^{j}(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\
&\quad (\forall j \in [0,i'))(\rho^{j}(\rho^{i}(t)) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\
&\quad exec(s_t, i) \in \|P\|_K \wedge \\
&\quad exec(s_{\rho^{i}(t)}, i') \in \|Q\|_K)
\end{aligned}
$$

$\iff$ by def. of ρ

$$
\begin{aligned}
&(\exists i \geq 0)(\exists i' \geq 0)(\\
&\quad t' = \rho^{i+i'}(t) \wedge \\
&\quad (\forall j \in [0,i))(\rho^{j}(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\
&\quad (\forall j \in [0,i'))(\rho^{i+j}(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\
&\quad exec(s_t, i) \in \|P\|_K \wedge \\
&\quad exec({s_t}^{i}, i') \in \|Q\|_K)
\end{aligned}
$$

$\iff$

$$
\begin{aligned}
&(\exists i \geq 0)(\exists i' \geq 0)(\\
&\quad t' = \rho^{i+i'}(t) \wedge \\
&\quad (\forall j \in [0,i))(\rho^{j}(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\
&\quad (\forall j \in [i,i+i'))(\rho^{j}(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\
&\quad exec(s_t, i) \in \|P\|_K \wedge \\
&\quad exec({s_t}^{i}, i') \in \|Q\|_K)
\end{aligned}
$$

$\iff$

$$
\begin{aligned}
&(\exists i \geq 0)(\exists i' \geq 0)(\\
&\quad t' = \rho^{i+i'}(t) \wedge \\
&\quad (\forall j \in [0,i+i'))(\rho^{j}(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\
&\quad exec(s_t, i) \in \|P\|_K \wedge \\
&\quad exec({s_t}^{i}, i') \in \|Q\|_K)
\end{aligned}
$$

$\iff$ by Lemma B.1

$$
\begin{aligned}
&(\exists i \geq 0)(\exists i' \geq 0)(\\
&\quad t' = \rho^{i+i'}(t) \wedge \\
&\quad (\forall j \in [0,k+k'))(\rho^{j}(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\
&\quad exec(s_t, i+i') \in \|P\|_K ; \|Q\|_K)
\end{aligned}
$$

$\iff$ because $i + i' = n$

$$(\exists n \geq 0)(\\ t' = \rho^n(t) \wedge \\ (\forall j \in [0, n))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ exec(s_t, n) \in \|P\|_K\,;\|Q\|_K)$$

■

Lemma B.7 *Let $K = \langle S, \tilde{A}, S_0, \tilde{P}\rangle$ be a Kripke structure for the signature Σ, and let $\mathfrak{A}$ be a full infinite closure fork algebra on $S, \tilde{A}$, extended with constants. If $t \in \mathcal{T}(S, T)$, then*

$$t \in \mathsf{ran}\,(\pi \nabla (\mathbf{A_i} \otimes \rho)) \iff \langle s_{t0}, s_{t1}\rangle \in \mathbf{A_i}$$

Proof.

$$t \in \mathsf{ran}\,(\pi \nabla (\mathbf{A_i} \otimes \rho))$$

$\iff$ by def. of ran

$$(\exists t' \in \mathcal{T}(S, T))(\langle t', t\rangle \in \pi \nabla (\mathbf{A_i} \otimes \rho))$$

$\iff$ by def. of ∇ and $\otimes$

$$(\exists t' \in \mathcal{T}(S, T))(\exists x, y, z)(\\ t = x \star (y \star z) \wedge \langle t', x\rangle \in \pi \wedge \langle t', y\rangle \in \pi\,;\mathbf{A_i} \wedge \langle t', z\rangle \in \rho;\rho)$$

$\iff$ by def. of π and ρ

$$(\exists t' \in \mathcal{T}(S, T))(\exists x, y, z)(\\ t = x \star (y \star z) \wedge x = \pi(t') \wedge \langle t', y\rangle \in \pi\,;\mathbf{A_i} \wedge z = \rho(\rho(t')))$$

$\iff$ by def. of ;

$$(\exists t' \in \mathcal{T}(S, T))(\exists x, y, z)(\\ t = x \star (y \star z) \wedge x = \pi(t') \wedge z = \rho(\rho(t')) \wedge \\ (\exists y')(\langle t', y'\rangle \in \pi \wedge \langle y', y\rangle \in \mathbf{A_i})))$$

$\Longleftrightarrow$ by def. of π

$$(\exists t' \in \mathcal{T}(S,T))(\exists x,y,z)(\\ t = x \star (y \star z) \wedge x = \pi(t') \wedge z = \rho(\rho(t'))\wedge \\ (\exists y')(y' = \pi(t') \wedge \langle y', y\rangle \in \mathbf{A_i})))$$

$\Longleftrightarrow$ because $x = \pi(t')$ and $z = \rho(\rho(t'))$

$$(\exists t' \in \mathcal{T}(S,T)) \\ (\exists y)(t = \pi(t') \star (y \star \rho(\rho(t')))\wedge \\ (\langle \pi(t'), y\rangle \in \mathbf{A_i}))$$

$\Longleftrightarrow$ because $y = \pi(\rho(t))$

$$(\exists t' \in \mathcal{T}(S,T)) \\ (\pi(t') = \pi(t) \wedge \rho(\rho(t')) = \rho(\rho(t)) \wedge (\langle \pi(t'), \pi(\rho(t))\rangle \in \mathbf{A_i}))$$

$\Longleftrightarrow$ because $\pi(t') = \pi(t)$

$$(\exists t' \in \mathcal{T}(S,T)) \\ (\pi(t') = \pi(t) \wedge \rho(\rho(t')) = \rho(\rho(t)) \wedge (\langle \pi(t), \pi(\rho(t))\rangle \in \mathbf{A_i}))$$

$\Longleftrightarrow$

$$\langle \pi(t), \pi(\rho(t))\rangle \in \mathbf{A_i}$$

$\Longleftrightarrow$ by def. of s_t, π and ρ

$$\langle (s_t)_0, (s_t)_1\rangle \in \mathbf{A_i}$$

■

Lemma B.8 *Let $K = \langle S, \tilde{A}, S_0, \tilde{P}\rangle$ be a Kripke structure for the signature Σ, and let $\mathfrak{A}$ be a full infinite fork algebra on S and $\tilde{A}$, extended with constants. If $t, t' \in \mathcal{T}(S,T)$, $\alpha \in ForDLTL(\Sigma)$ and $R \in PrgDLTL(\Sigma)$, then*

$(\forall k \in I\!N)($

$$\langle t, t' \rangle \in M_{DLTL}(\alpha, R)^{;k}$$

$$\iff$$

$$(\exists i \geq 0)(\\ t' = \rho^i(t) \wedge \\ (\forall j \in [0, i))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ exec(s_t, i) \in \|R\|_K{}^{;k}))$$

Proof. The proof follows by induction on k.

- base case)

$$\langle t, t' \rangle \in M_{DLTL}(\alpha, R)^{;0}$$

$\iff$ by def. 2.33

$$\langle t, t' \rangle \in \mathbf{1}'$$

$\iff$ by def. of $\mathbf{1}'$

$$t = t'$$

$\iff$ by def. 5.5

$$t = t' \wedge \lambda \in \|R\|_K{}^{;0}$$

$\iff$ by def. of *exec*

$$t = t' \wedge exec(s_t, 0) \in \|R\|_K{}^{;0}$$

$\iff$ by def. of ρ

$$t' = \rho^0(t) \wedge \\ (\forall j \in [0, 0))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ exec(s_t, 0) \in \|R\|_K{}^{;0}$$

$\iff$

$$(\exists i \geq 0)(\\ t' = \rho^i(t) \wedge \\ (\forall j \in [0, i))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ exec(s_t, i) \in \|R\|_K{}^{;0})$$

- inductive step)

$$\langle t, t'\rangle \in M_{DLTL}(\alpha, R)^{;k+1}$$

$\Longleftrightarrow$ by def. 2.33

$$\langle t, t'\rangle \in M_{DLTL}(\alpha, R); M_{DLTL}(\alpha, R)^{;k}$$

$\Longleftrightarrow$ by def. of ;

$$(\exists t'')(\langle t, t''\rangle \in M_{DLTL}(\alpha, R) \wedge \langle t'', t'\rangle \in M_{DLTL}(\alpha, R)^{;k})$$

$\Longleftrightarrow$ by Ind. Hyp.

$$\begin{array}{l} (\exists t'')(\\ \quad (\exists i \geq 0)(\\ \quad\quad t'' = \rho^i(t) \wedge \\ \quad\quad (\forall j \in [0, i))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad\quad exec(s_t, i) \in \|R\|_K) \wedge \\ \quad (\exists i' \geq 0)(\\ \quad\quad t = \rho^i(t'') \wedge \\ \quad\quad (\forall j \in [0, i))(\rho^j(t'') \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad\quad exec(s_{t''}, i) \in \|R\|_K{}^{;k})) \end{array}$$

$\Longleftrightarrow$ by independence of t'', i, i'

$$\begin{array}{l} (\exists i \geq 0)(\exists i' \geq 0)(\exists t'')(\\ \quad t'' = \rho^i(t) \wedge \\ \quad (\forall j \in [0, i))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad exec(s_t, i) \in \|R\|_K \wedge \\ \quad t = \rho^i(t'') \wedge \\ \quad (\forall j \in [0, i))(\rho^j(t'') \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad exec(s_{t''}, i) \in \|R\|_K{}^{;k}) \end{array}$$

$\Longleftrightarrow$ by Lemma B.6

$$\begin{array}{l} (\exists n \geq 0)(\\ \quad t = \rho^n(t) \wedge \\ \quad (\forall j \in [0, n))(\rho^j(t'') \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad exec(s_t, n) \in \|R\|_K; (\|R\|_K{}^{;k})) \end{array}$$

$\Longleftrightarrow$ by def. 2.33

$$\begin{array}{l} (\exists n \geq 0)(\\ \quad t = \rho^n(t) \wedge \\ \quad (\forall j \in [0, n))(\rho^j(t'') \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad exec(s_t, n) \in \|R\|_K{}^{;k+1}) \end{array}$$

■

Lemma B.9 *Let $K = \langle S, \tilde{A}, S_0, \tilde{P} \rangle$ be a Kripke structure for the signature Σ, and let $\mathfrak{A}$ be a full infinite closure fork algebra on S and $\tilde{A}$, extended with constants. If $\alpha \in ForDLTL(\Sigma)$, $R \in PrgDLTL(\Sigma)$ and $t, t' \in \mathcal{T}(S, T)$, then*

$$\begin{array}{ll} & \langle t, t' \rangle \in M_{DLTL}(\alpha, R) \\ \iff & \\ & (\exists i \geq 0)(\\ & \quad t' = \rho^i(t) \wedge \\ & \quad (\forall j \in [0, i))(\rho^i(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ & \quad exec(s_t, i) \in \|R\|_K) \end{array}$$

Proof. The proof of this lemma follows by induction on the structure of program R.

- $R = a_k$

$$\begin{array}{ll} & \langle t, t' \rangle \in M_{DLTL}(\alpha, a_k) \\ \iff & \text{by def. of } M_{DLTL}(\alpha, P) \\ & \langle t, t' \rangle \in Dom\,(T_{DLTL}\,(\alpha))\,; Ran\,(\pi \nabla (\mathbf{A_k} \otimes \rho))\,; \rho \\ \iff & \text{by def. of } ; \\ & (\exists r)(\exists r')(\\ & \quad \langle t, r \rangle \in Dom\,(T_{DLTL}\,(\alpha)) \wedge \\ & \quad \langle r, r' \rangle \in Ran\,(\pi \nabla (\mathbf{A_k} \otimes \rho)) \wedge \\ & \quad \langle r', t' \rangle \in \rho) \\ \iff & \text{since } Dom \leq \mathbf{1'} \text{ and } Ran \leq \mathbf{1'} \\ & \langle t, t \rangle \in Dom\,(T_{DLTL}\,(\alpha)) \wedge \\ & \langle t, t \rangle \in Ran\,(\pi \nabla (\mathbf{A_k} \otimes \rho)) \wedge \\ & \langle t, t' \rangle \in \rho \\ \iff & \text{by def. of } Dom \text{ and } Ran \\ & t \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)) \wedge t \in \mathsf{ran}\,(\pi \nabla (\mathbf{A_k} \otimes \rho)) \wedge \langle t, t' \rangle \in \rho \\ \iff & \text{by def. of } \rho \\ & t \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)) \wedge t \in \mathsf{ran}\,(\pi \nabla (\mathbf{A_k} \otimes \rho)) \wedge t' = \rho^1(t) \\ \iff & \text{by Lemma B.7} \\ & t \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)) \wedge \langle s_{t0}, s_{t1} \rangle \in \mathbf{A_k} \wedge t' = \rho^1(t) \end{array}$$

$\Longleftrightarrow$ since $\mathbf{A_k} = \tilde{a_k}$

$$t \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)) \wedge \langle s_{t0}, s_{t1}\rangle \in \tilde{a_k} \wedge t' = \rho^1(t)$$

$\Longleftrightarrow$ by def. 5.6

$$t' = \rho^1(t) \wedge t \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)) \wedge \langle s_{t0}, s_{t1}\rangle \in \|a_k\|_K$$

$\Longleftrightarrow$ by def. 5.7

$$t' = \rho^1(t) \wedge t \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)) \wedge exec(s_t, 1) \in \|a_k\|_K$$

$\Longleftrightarrow$ by def. of ρ

$$t' = \rho^1(t) \wedge \rho^0(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)) \wedge exec(s_t, 1) \in \|a_k\|_K$$

$\Longleftrightarrow$

$$\begin{array}{l} t' = \rho^1(t) \wedge \\ (\forall j \in [0,1))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ exec(s_t, 1) \in \|a_k\|_K \end{array}$$

$\Longleftrightarrow$

$$\begin{array}{l} (\exists i \geq 0)(\\ \quad t' = \rho^i(t) \wedge \\ \quad (\forall j \in [0,i))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad exec(s_t, i) \in \|a_k\|_K) \end{array}$$

- $R = P \cup Q$

$$\langle t, t'\rangle \in M_{DLTL}(\alpha, P \cup Q)$$

$\Longleftrightarrow$by def. of $M_{DLTL}(\alpha, P)$

$$\langle t, t'\rangle \in M_{DLTL}(\alpha, P) \cup M_{DLTL}(\alpha, Q)$$

$\Longleftrightarrow$by set theory

$$\langle t, t'\rangle \in M_{DLTL}(\alpha, P) \vee \langle t, t'\rangle \in M_{DLTL}(\alpha, Q)$$

$\Longleftrightarrow$ by Ind. Hyp.

$$
\begin{aligned}
&(\exists i \geq 0)(\\
&\quad t' = \rho^i(t) \wedge\\
&\quad (\forall j \in [0, i))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge\\
&\quad exec(s_t, i) \in \|P\|_K)\\
&\vee\\
&(\exists i' \geq 0)(\\
&\quad t' = \rho^{i'}(t) \wedge\\
&\quad (\forall j' \in [0, i'))(\rho^{j'}(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge\\
&\quad exec(s_t, i') \in \|Q\|_K)
\end{aligned}
$$

$\Longleftrightarrow$

$$
\begin{aligned}
&(\exists i \geq 0)(\\
&\quad t' = \rho^i(t) \wedge\\
&\quad (\forall j \in [0, i))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge\\
&\quad (exec(s_t, i) \in \|P\|_K \vee exec(s_t, i) \in \|Q\|_K))
\end{aligned}
$$

$\Longleftrightarrow$ by set theory

$$
\begin{aligned}
&(\exists i \geq 0)(\\
&\quad t' = \rho^i(t) \wedge\\
&\quad (\forall j \in [0, i))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge\\
&\quad exec(s_t, i) \in \|P\|_K \cup \|Q\|_K)
\end{aligned}
$$

$\Longleftrightarrow$ by def. 5.6

$$
\begin{aligned}
&(\exists i \geq 0)(\\
&\quad t' = \rho^i(t) \wedge\\
&\quad (\forall j \in [0, i))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge\\
&\quad exec(s_t, i) \in \|P \cup Q\|_K)
\end{aligned}
$$

- $R = P; Q$

$$\langle t, t' \rangle \in M_{DLTL}(\alpha, P; Q)$$

$\iff$ by def. of M_{DLTL}

$$\langle t, t' \rangle \in M_{DLTL}(\alpha, P); M_{DLTL}(\alpha, Q)$$

$\iff$ by def. of ;

$$\begin{array}{l} (\exists t'')(\\ \quad \langle t, t'' \rangle \in M_{DLTL}(\alpha, P) \wedge \\ \quad \langle t'', t' \rangle \in M_{DLTL}(\alpha, Q)) \end{array}$$

$\iff$ by Ind. Hyp.

$$\begin{array}{l} (\exists t'')(\\ \quad (\exists i \geq 0)(\\ \quad\quad t'' = \rho^i(t) \wedge \\ \quad\quad (\forall j \in [0, i))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad\quad exec(s_t, i) \in \|P\|_K) \wedge \\ \quad (\exists i' \geq 0)(\\ \quad\quad t' = \rho^{i'}(t'') \wedge \\ \quad\quad (\forall j' \in [0, i'))(\rho^{j'}(t'') \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)))) \wedge \\ \quad\quad exec(s_{t''}, i') \in \|Q\|_K) \end{array}$$

$\iff$

$$\begin{array}{l} (\exists i \geq 0)(\exists i' \geq 0)(\exists t'')(\\ \quad t'' = \rho^i(t) \wedge \\ \quad (\forall j \in [0, i))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad exec(s_t, i) \in \|P\|_K \wedge \\ \quad t' = \rho^{i'}(t'') \wedge \\ \quad (\forall j' \in [0, i'))(\rho^{j'}(t'') \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad exec(s_{t''}, i') \in \|Q\|_K) \end{array}$$

$\iff$ by Lemma B.6

$$\begin{array}{l} (\exists n \geq 0)(\\ \quad t' = \rho^n(t) \wedge \\ \quad (\forall j \in [0, n))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad exec(s_t, n) \in \|P; Q\|_K) \end{array}$$

- $R = P^*$

$$\langle t, t' \rangle \in M_{DLTL}(\alpha, P^*)$$

$\iff$ by def. of M_{DLTL}

$$\langle t, t' \rangle \in M_{DLTL}(\alpha, P)^*$$

$\iff$ by def. of *

$$(\exists k \in [0, \infty))(\langle t, t' \rangle \in M_{DLTL}(\alpha, P)^{;k})$$

$\iff$ by Lemma B.8

$$\begin{array}{l} (\exists k \in [0, \infty))(\exists n \geq 0)(\\ \quad t = \rho^n(t) \wedge \\ \quad (\forall j \in [0, n))(\rho^j(t'') \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad exec(s_t, n) \in \|P\|_K{}^{;k}) \end{array}$$

$\iff$

$$\begin{array}{l} (\exists n \geq 0)(\\ \quad t' = \rho^n(t) \wedge \\ \quad (\forall j \in [0, n))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad (\exists k \in [0, \infty))(exec(s_t, n) \in \|P\|_K{}^{;k})) \end{array}$$

$\iff$ by def. of *

$$\begin{array}{l} (\exists n \geq 0)(\\ \quad t' = \rho^n(t) \wedge \\ \quad (\forall j \in [0, n))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad exec(s_t, n) \in \|P\|_K{}^*) \end{array}$$

$\iff$ by def. 5.6

$$\begin{array}{l} (\exists n \geq 0)(\\ \quad t' = \rho^n(t) \wedge \\ \quad (\forall j \in [0, n))(\rho^j(t) \in \mathsf{dom}\,(T_{DLTL}\,(\alpha))) \wedge \\ \quad exec(s_t, n) \in \|P^*\|_K) \end{array}$$

■

Finally, we present the proofs for lemmas previously introduced in section 5.

Lemma B.10 *Given* $\mathfrak{A} \in \mathsf{PCFA}$ *extended with constants* $\mathbf{S}$, $\mathbf{T}$, $\mathbf{S_0}$, $\mathbf{tr}$, $\{\mathbf{A_i}\}_{i \in \mathcal{A}}$ *and* $\{\mathbf{P_i}\}_{i \in \mathcal{P}}$ *satisfying Axs. (16)-(26), there exists a Kripke structure* K *such that for all* $t \in \mathsf{dom}\,(\mathbf{tr})$,

$$t \in \mathsf{dom}\,(T_{DLTL}\,(\alpha)) \iff K, s_t \models_{DLTL} \alpha\ .$$

Proof. Let us define the Kripke structure $K = \langle S, \tilde{A}, S_0, \tilde{P} \rangle$ as follows:

- $S = \mathsf{dom}\,(\mathbf{S})$
- $\tilde{a_i} = \mathbf{A_i}$ for all $i \in \mathcal{A}$
- $S_0 = \mathsf{dom}\,(\mathbf{S_0})$,
- $\tilde{p_i} = \{s | s \in \mathsf{dom}\,(\mathbf{P_i})\}$ for all $i \in \mathcal{P}$

The proof follows by induction on the structure of the formula α.

- $\alpha = p_i$, for $i \in \mathcal{P}$:

$$
\begin{aligned}
& t \in \mathsf{dom}\,(T_{DLTL}\,(p_i)) & \\
\Longleftrightarrow\, & t \in \mathsf{dom}\,(\pi\,;\mathbf{P_i}) & \text{(by def. of } T_{DLTL}\,(\alpha)) \\
\Longleftrightarrow\, & \pi(t) \in \mathsf{dom}\,(\mathbf{P_i}) & \text{(by set theory)} \\
\Longleftrightarrow\, & s_{t0} \in \mathsf{dom}\,(\mathbf{P_i}) & \text{(by def. of } s_t) \\
\Longleftrightarrow\, & s_{t0} \in \tilde{p_i} & \text{(by def. of } K) \\
\Longleftrightarrow\, & K, s_t \models_{DLTL} p_i & \text{(by def. of } \models_{DLTL})
\end{aligned}
$$

- $\alpha = \neg\beta$:

$$
\begin{aligned}
& t \in \mathsf{dom}\,(T_{DLTL}\,(\neg\beta)) & \\
\Longleftrightarrow\, & t \in \mathsf{dom}\left(\mathbf{tr}\,;\overline{T_{DLTL}\,(\beta)}\right) & \text{(by def. of } T_{DLTL}\,(\alpha)) \\
\Longleftrightarrow\, & t \in \mathsf{dom}\,(\mathbf{tr}) \vee t \notin \mathsf{dom}\,(T_{DLTL}\,(\beta)) & \\
& & \text{(by set theory and } T_{DLTL}\,(\alpha) \text{ yields right-ideals)} \\
\Longleftrightarrow\, & K, s_t \not\models_{DLTL} \beta & \text{(by Ind. Hyp.)} \\
\Longleftrightarrow\, & K, s_t \models_{DLTL} \neg\beta\ . & \text{(by def. of } \models_{DLTL})
\end{aligned}
$$

- $\alpha = \beta \vee \gamma$:

$$
\begin{aligned}
& t \in \mathsf{dom}\,(T_{DLTL}\,(\beta \vee \gamma)) & \\
\Longleftrightarrow\, & t \in \mathsf{dom}\,(T_{DLTL}\,(\beta) + T_{DLTL}\,(\gamma)) & \text{(by def. of } T_{DLTL}\,(\alpha)) \\
\Longleftrightarrow\, & t \in \mathsf{dom}\,(T_{DLTL}\,(\beta)) \vee t \in \mathsf{dom}\,(T_{DLTL}\,(\gamma)) & \\
& & \text{(by set theory and } T_{DLTL}\,(\alpha) \text{ yields right-ideals)} \\
\Longleftrightarrow\, & K, s_t \models_{DLTL} \beta \vee K, s_t \models_{DLTL} \gamma & \text{(by Ind. Hyp.)} \\
\Longleftrightarrow\, & K, s_t \models_{DLTL} \beta \vee \gamma\ . & \text{(by def. if } \models_{DLTL})
\end{aligned}
$$

- $\alpha = \beta \, \mathsf{U}^P \, \gamma$:

$$
\begin{aligned}
& t \in \mathsf{dom}\left(T_{DLTL}\left(\beta \, \mathsf{U}^P \, \gamma\right)\right) \\
\iff & \text{by def. of } T_{DLTL}(\alpha) \\
& t \in \mathsf{dom}\left(M_{DLTL}(\beta, P);T_{DLTL}(\gamma)\right) \\
\iff & \text{by def. of ;} \\
& (\exists t')(\langle t, t' \rangle \in M_{DLTL}(\beta, P) \wedge t' \in \mathsf{dom}\left(T_{DLTL}(\gamma)\right)) \\
\iff & \text{by Lemma B.9} \\
& (\exists t')(\exists i \geq 0)(\\
& \quad t' = \rho^i(t) \wedge \\
& \quad (\forall j \in [0, i))(\rho^j(t) \in \mathsf{dom}\left(T_{DLTL}(\beta)\right)) \wedge \\
& \quad exec(s_t, i) \in \|P\|_K \wedge \\
& \quad t' \in \mathsf{dom}\left(T_{DLTL}(\gamma)\right)) \\
\iff & \\
& (\exists i \geq 0)(\\
& \quad \rho^i(t) \in \mathsf{dom}\left(T_{DLTL}(\gamma)\right) \wedge \\
& \quad (\forall j \in [0, i))(\rho^j(t) \in \mathsf{dom}\left(T_{DLTL}(\beta)\right)) \wedge \\
& \quad exec(s_t, i) \in \|P\|_K) \\
\iff & \text{by Ind. Hyp.} \\
& (\exists i \geq 0)(\\
& \quad K, s_{\rho^i(t)} \models_{DLTL} \gamma \wedge \\
& \quad (\forall j \in [0, i))(K, s_{\rho^j(t)} \models_{DLTL} \beta) \wedge \\
& \quad exec(s_t, i) \in \|P\|_K) \\
\iff & \text{by def. of } s_t \\
& (\exists i \geq 0)(\\
& \quad K, (s_t)^i \models_{DLTL} \gamma \wedge \\
& \quad (\forall j \in [0, i))(K, (s_t)^j \models_{DLTL} \beta) \wedge \\
& \quad exec(s_t, i) \in \|P\|_K) \\
\iff & \text{def } \models_{DLTL} \\
& K, s_t \models_{DLTL} \beta \, \mathsf{U}^P \, \gamma
\end{aligned}
$$

■

Lemma B.11 *Given a Kripke structure $K = \langle S, \tilde{A}, S_0, \tilde{P}\rangle$, there exists a non empty class of proper closure fork algebras extended with constants* $\mathbf{S}$, $\mathbf{T}$, $\mathbf{S_0}$, $\mathbf{tr}$, $\{\mathbf{A_i}\}_{i\in\mathcal{A}}$ *and* $\{\mathbf{P_i}\}_{i\in\mathcal{P}}$*, such that, for all* $\mathfrak{A}$ *in this class,*

- $\mathfrak{A}$ *satisfies Axs. (16)-(26)*
- *for all* $s \in \Delta_K$,

$$K, s \models_{DLTL} \alpha \Longleftrightarrow t_s \in \mathsf{dom}\left(T_{DLTL}\left(\alpha\right)\right).$$

Proof. Let $\mathfrak{A} \in \mathsf{PCFA}$, such that,

- $\mathfrak{A}$ is a full infinite closure fork algebra on S and $\tilde{A}$, extended with constants.
- $\mathbf{S_0} = \{\langle s, s\rangle \,|\, s \in S_0\}$
- $\mathsf{dom}\left(\mathbf{P_i}\right) = \tilde{p_i}$ for all $i \in \mathcal{P}$

Since $\mathfrak{A}$ is a full infinite closure fork algebra, $\mathfrak{A}$ satisfies the axioms of ω-CCFA^{+DLTL}.
The proof of this lemma follows by induction on the structure of formula α.

- $\alpha = p_i$:

$$\begin{aligned}
& K, s \models_{DLTL} p_i && \\
\Longleftrightarrow\ & s_0 \in \tilde{p_i} && \text{(by def. of } \models_{DLTL}\text{)}\\
\Longleftrightarrow\ & s_0 \in \mathsf{dom}\left(\mathbf{P_i}\right) && \text{(by def. of } \mathbf{P_i}\text{)}\\
\Longleftrightarrow\ & \pi(t_s) \in \mathsf{dom}\left(\mathbf{P_i}\right) && \text{(by def. of } t_s\text{)}\\
\Longleftrightarrow\ & t_s \in \mathsf{dom}\left(\pi ; \mathbf{P_i}\right) && \text{(by set theory)}\\
\Longleftrightarrow\ & t_s \in \mathsf{dom}\left(T_{DLTL}\left(p_i\right)\right) && \text{(by def. of } T_{DLTL}\text{)}
\end{aligned}$$

- $\alpha = \neg\beta$:

$$\begin{aligned}
& K, s \models_{DLTL} \neg\beta && \\
\Longleftrightarrow\ & K, s \not\models_{DLTL} \beta && \text{(by def. of } \models_{DLTL}\text{)}\\
\Longleftrightarrow\ & t_s \notin \mathsf{dom}\left(T_{DLTL}\left(\beta\right)\right) && \text{(by Ind. Hyp.)}\\
\Longleftrightarrow\ & t_s \in \mathsf{dom}\left(\mathbf{tr}\right) \wedge t_s \notin \mathsf{dom}\left(T_{DLTL}\left(\beta\right)\right) && \text{(by def. of } t_s\text{)}\\
\Longleftrightarrow\ & t_s \in \mathsf{dom}\left(\mathbf{tr} ; \overline{T_{DLTL}\left(\beta\right))}\right) && \\
& && \text{(by set theory, def. } \mathbf{tr} \text{ and } T_{DLTL} \text{ yields right-ideals)}\\
\Longleftrightarrow\ & t_s \in \mathsf{dom}\left(T_{DLTL}\left(\neg\beta\right)\right) && \text{(by def. of } T_{DLTL}\text{)}
\end{aligned}$$

- $\alpha = \beta \vee \gamma$

$$
\begin{aligned}
& K, s \models_{DLTL} \beta \vee \gamma \\
\Longleftrightarrow & K, s \models_{DLTL} \beta \vee K, s \models_{DLTL} \gamma && \text{(by def. of } \models_{DLTL}\text{)} \\
\Longleftrightarrow & t_s \in \mathsf{dom}\,(T_{DLTL}\,(\beta)) \vee t_s \in \mathsf{dom}\,(T_{DLTL}\,(\gamma)) && \text{(by Ind. Hyp.)} \\
\Longleftrightarrow & t_s \in \mathsf{dom}\,(T_{DLTL}\,(\beta) + T_{DLTL}\,(\gamma)) \\
& && \text{(by set theory and } T_{DLTL} \text{ yields right-ideals)} \\
\Longleftrightarrow & t_s \in \mathsf{dom}\,(T_{DLTL}\,(\beta \vee \gamma)) && \text{(by def. of } T_{DLTL}\text{)}
\end{aligned}
$$

- $\alpha = \beta \mathsf{U}^P \gamma$

$$K, s \models_{DLTL} \beta \mathsf{U}^P \gamma$$

$\iff$ by def. of $\models_{DLTL}$

$$\begin{array}{l}(\exists i \geq 0)(\\ \quad K, s^i \models_{DLTL} \gamma \wedge \\ \quad (\forall j \in [0, i))(K, s^j \models_{DLTL} \beta) \wedge \\ \quad exec(s, i) \in \|P\|_K)\end{array}$$

$\iff$ by Ind. Hyp.

$$\begin{array}{l}(\exists i \geq 0)(\\ \quad t_{s^i} \in \mathsf{dom}\,(T_{DLTL}\,(\gamma)) \wedge \\ \quad (\forall j \in [0, i))(t_{s^j} \in \mathsf{dom}\,(\beta)) \wedge \\ \quad exec(s, i) \in \|P\|_K)\end{array}$$

$\iff$ by def. of t_s

$$\begin{array}{l}(\exists i \geq 0)(\\ \quad \rho^i(t_s) \in \mathsf{dom}\,(T_{DLTL}\,(\gamma)) \wedge \\ \quad (\forall j \in [0, i))(\rho^j(t_s) \in \mathsf{dom}\,(\beta)) \wedge \\ \quad exec(s_{t_s}, i) \in \|P\|_K)\end{array}$$

$\iff$

$$\begin{array}{l}(\exists t')(\exists i \geq 0)(\\ \quad t' = \rho^i(t_s) \wedge \\ \quad (\forall j \in [0, i))(\rho^j(t_s) \in \mathsf{dom}\,(\beta)) \wedge \\ \quad exec(s_{t_s}, i) \in \|P\|_K \wedge \\ \quad t' \in \mathsf{dom}\,(T_{DLTL}\,(\gamma)))\end{array}$$

$\iff$ by Lemma B.9

$$(\exists t')(\langle t_s, t' \rangle \in M_{DLTL}(\beta, P) \wedge t' \in \mathsf{dom}\,(T_{DLTL}\,(\gamma)))$$

$\iff$ by def. of ;
$t_s \in \mathsf{dom}\,(M_{DLTL}(\beta, P); T_{DLTL}\,(\gamma))$

$\iff$ by def. of T_{DLTL}

$$t_s \in \mathsf{dom}\left(T_{DLTL}\left(\beta \mathsf{U}^P \gamma\right)\right)$$

■

C Reasoning across formalisms: Laying foundations

In this appendix we lay some foundation to reason across PDL, LTL, and $DLTL$ using ω-CCFA^+.

Lemma C.1 *Let e be a fork algebra equation. Then,*

$$\models_{\omega\text{-}\mathsf{CCFA}^+} e \iff \vdash_{\omega\text{-}\mathsf{CCFA}^+} e$$

Proof.

$\Longrightarrow$)

$$\begin{aligned} \models_{\omega\text{-}\mathsf{CCFA}^+} e &\Longrightarrow EqTh(\omega\text{-}\mathsf{CFA}^+) \models_{\omega\text{-}\mathsf{CCFA}^+} e && \text{(by def. } \omega\text{-}\mathsf{CFA}^+\text{)} \\ &\Longrightarrow EqTh(\omega\text{-}\mathsf{CFA}^+) \vdash_{\omega\text{-}\mathsf{CCFA}^+} e && \text{(by completeness of eq. logic)} \end{aligned}$$

Notice that an equational proof e from $EqTh(\omega\text{-}\mathsf{CFA}^+)$ will be a finite height tree (probably with infinite width) whose leaves are equations in $EqTh(\omega\text{-}\mathsf{CFA}^+)$. In order to show that $\vdash_{\omega\text{-}\mathsf{CCFA}^+} e$, it suffices to replace each leaf in $EqTh(\omega\text{-}\mathsf{CFA}^+)$ by its corresponding proof in ω-CCFA^+.

$\Longleftarrow$) This implication follows directly from the definition of ω-CFA

■

In the next lemma, we state that every PDL test free program is a DLTL program and viceversa.

Lemma C.2 *Let Σ be a signature.*

$$R \in FreePrgPDL(\Sigma) \iff R \in PrgDLTL(\Sigma)$$

Proof. It follows by induction on the program structure. ■

The next lemma states that, given a program P, there is a $DLTL$ formula to single out those traces which begin with a trace prefix from $\|P\|_K$.

Lemma C.3 *Let K be a Kripke structure for the logic $DLTL(\Sigma)$. Let $R \in PrgDLTL(\Sigma)$, and $s \in \Delta_K$,*

$$(\exists k \in [0,\infty))(exec(s,k) \in \|R\|_K) \iff K, s \models_{DLTL} \textbf{true}\ \mathsf{U}^R\ \textbf{true}$$

Proof.

$$(\exists k \in [0,\infty))(exec(s,k) \in \|R\|_K))$$

$\iff$ by def. of $\models_{DLTL}$

$$(\exists k \in [0,\infty))(\\ K, s^k \models_{DLTL} \textbf{true} \wedge \\ (\forall j \in [0,k))(K, s^j \models_{DLTL} \textbf{true})) \wedge \\ exec(s,k) \in \|R\|_K)$$

$\iff$ by def. of $\models_{DLTL}$

$$K, s \models_{DLTL} \textbf{true} \ \mathsf{U}^R \ \textbf{true}$$

■

Lemma C.4 *Given a Kripke structure K for the logic $DLTL$,*

$$\mathfrak{C}_K \subseteq \mathfrak{C}_{K^{LTL}}$$

Proof. Let $\mathfrak{A} \in \mathfrak{C}_K$,

- $\mathfrak{A}$ is a proper closure fork algebra extended with constants.
- $\mathfrak{A}$ satisfies Axs. (16)-(26), therefore, $\mathfrak{A}$ satisfies Axs. (16)-(18) and Axs. (20)-(25).
- We have to prove that

$$K^{LTL}, s \models_{LTL} \alpha \iff t_s \in \mathsf{dom}\,(T_{LTL}(\alpha))$$

for all $s \in \Delta_{K^{LTL}}$, $\alpha \in ForLTL(P)$.

$$\begin{aligned} & K^{LTL}, s \models_{LTL} \alpha \\ \iff & K, s \models_{DLTL} T_{LTL\to DLTL}(\alpha) && \text{(by Thm. 5.1)} \\ \iff & t_s \in \mathsf{dom}\,(T_{DLTL}\,(T_{LTL\to DLTL}(\alpha))) && \text{(by } \mathfrak{A} \in \mathfrak{C}_{DLTL}) \\ \iff & t_s \in \mathsf{dom}\,(\mathbf{tr}; T_{DLTL}\,(T_{LTL\to DLTL}(\alpha))) && \text{(since } t_s \in \mathsf{dom}\,(\mathbf{tr})) \\ \iff & t_s \in \mathsf{dom}\,(\mathbf{tr}; T_{LTL}(\alpha)) && \text{(by Lemma D.8)} \\ \iff & t_s \in \mathsf{dom}\,(T_{LTL}(\alpha)) \end{aligned}$$

■

Lemma C.5 *Given a Kripke structure K for the logic $DLTL$,*

$$\mathfrak{C}_K \subseteq \mathfrak{C}_{K^{PDL}}$$

Proof. Let $\mathfrak{A} \in \mathfrak{C}_K$,

- $\mathfrak{A}$ is a proper closure fork algebra extended with constants.
- $\mathfrak{A}$ satisfies Axs. (16)-(26), therefore, $\mathfrak{A}$ satisfies Axs. (16)-(19).
- We have to prove that

$$K^{PDL}, q \models_{PDL} \alpha \iff q \in \mathsf{dom}\,(T_{PDL}(\alpha))$$

for all $q \in S$, $\alpha \in ForPDL(\Sigma)$. We prove this by induction on formula α. Let $q \in S$,

  - $\alpha = p_i$

$$\begin{aligned} & K^{PDL}, q \models_{PDL} p_i \\ \iff & q \in \tilde{p_i} && \text{(by def. } \models_{PDL}) \\ \iff & (\forall s \in \Delta_K)(s_0 = q \Longrightarrow s_0 \in \tilde{p_i}) \\ \iff & (\forall s \in \Delta_K)(s_0 = q \Longrightarrow K, s \models_{DLTL} p_i) && \text{(by def. } \models_{DLTL}) \\ \iff & (\forall s \in \Delta_K)(\pi(t_s) = q \Longrightarrow t_s \in \mathsf{dom}\,(T_{DLTL}\,(p_i))) \\ & && \text{(by } \mathfrak{A} \in \mathfrak{C}_{DLTL}) \\ \iff & (\forall s \in \Delta_K)(\pi(t_s) = q \Longrightarrow t_s \in \mathsf{dom}\,(\pi;\mathbf{P_i})) && \text{(by def. } T_{DLTL}) \\ \iff & (\forall s \in \Delta_K)(\pi(t_s) = q \Longrightarrow \pi(t_s) \in \mathsf{dom}\,(\mathbf{P_i})) \\ \iff & (\forall s \in \Delta_K)(q \in \mathsf{dom}\,(\mathbf{P_i})) \\ \iff & q \in \mathsf{dom}\,(\mathbf{P_i}) \end{aligned}$$

  - $\alpha = \neg\beta$

$$\begin{aligned} & K^{PDL}, q \models_{PDL} \neg\beta \\ \iff & K^{PDL}, q \not\models_{PDL} \beta && \text{(by def. } \models_{PDL}) \\ \iff & q \notin \mathsf{dom}\,(T_{PDL}(\beta)) && \text{(by Ind. Hyp.)} \\ \iff & q \in \mathsf{dom}\left(\overline{T_{PDL}(\beta)}\right) && \text{(since } T_{PDL} \text{ is right ideal)} \\ \iff & q \in \mathsf{dom}\left(\mathbf{S};\overline{T_{PDL}(\beta)}\right) && \text{(since } q \in S) \\ \iff & q \in \mathsf{dom}\,(T_{PDL}(\neg\beta)) && \text{(by def. } T_{PDL}) \end{aligned}$$

  - $\alpha = \beta \vee \gamma$

$$\begin{aligned} & K^{PDL}, q \models_{PDL} \beta \vee \gamma \\ \iff & K^{PDL}, q \models_{PDL} \beta \vee K^{PDL}, q \models_{PDL} \gamma && \text{(by def. } \models_{PDL}) \\ \iff & q \in \mathsf{dom}\,(T_{PDL}(\beta)) \vee q \in \mathsf{dom}\,(T_{PDL}(\gamma)) && \text{(by Ind. Hyp.)} \\ \iff & q \in \mathsf{dom}\,(T_{PDL}(\beta)) \cup \mathsf{dom}\,(T_{PDL}(\gamma)) \\ \iff & q \in \mathsf{dom}\,(T_{PDL}(\beta) + T_{PDL}(\gamma)) \\ \iff & q \in \mathsf{dom}\,(T_{PDL}(\beta \vee \gamma)) && \text{(by def. } T_{PDL}) \end{aligned}$$

- $\alpha = \langle P \rangle \beta$

$$
\begin{aligned}
& K^{PDL}, q \models_{PDL} \langle P \rangle \beta \\
\iff & (\exists q')(\langle q, q' \rangle \in Prg_K(P)) \wedge (K^{PDL}, q' \models_{PDL} \beta) \\
& \qquad \text{(by def. } \models_{PDL}\text{)} \\
\iff & (\exists q')(\langle q, q' \rangle \in Prg_K(P)) \wedge (q' \in T_{PDL}(\beta)) \quad \text{(by Ind. Hyp.)} \\
\iff & (\exists q')(\langle q, q' \rangle \in M_{PDL}(P)) \wedge (q' \in T_{PDL}(\beta)) \quad \text{(by Lemma 3.2)} \\
\iff & q \in \mathsf{dom}\,(M_{PDL}(P); T_{PDL}(\beta)) \\
\iff & q \in \mathsf{dom}\,(T_{PDL}(\langle P \rangle \beta)) \quad \text{(by def. } T_{PDL}\text{)}
\end{aligned}
$$

■

D On Fork results for reasoning across formalisms

Lemma D.1 *For all $\alpha \in ForDLTL(\Sigma)$, $T_{DLTL}(\alpha)$ is right-ideal.*

Proof. It is easy to see from definition of T_{DLTL}. ■

By $1'^{k}$ we denote the relation $\underbrace{1' \otimes \ldots \otimes 1'}_{k \text{ times}}$.

Lemma D.2 *for all $k \geq 1$*

$$\vdash_{\omega\text{-CCFA}^+} \mathbf{tr} \leq 1'^{k}$$

Proof.

- base case:

$\leq$)

$$\begin{aligned} \mathbf{tr} &\leq \mathbf{S} \otimes \mathbf{tr} && \text{(by Ax. 24)} \\ &\leq 1' \otimes 1' && \text{(by Ax. 22, Ax. 16 and Lemma A.2.1)} \end{aligned}$$

- inductive step:

$$\begin{aligned} \mathbf{tr} &\leq \mathbf{S} \otimes \mathbf{tr} && \text{(by Ax. 24)} \\ &\leq 1' \otimes \mathbf{tr} && \text{(by Ax. 16 and Lemma A.2.1)} \\ &\leq 1' \otimes 1'^{k} && \text{(by Ind. Hyp. and Lemma A.2.1)} \\ &= 1'^{k+1} \end{aligned}$$

■

Lemma D.3

$$\vdash_{\omega\text{-CCFA}^+} \mathbf{tr} ; T_{DLTL}(\mathbf{true}) = \mathbf{tr} ; \mathbf{1}$$

Proof. Follows easily from Lemma D.1 ■

Lemma D.4

$$\vdash_{\omega\text{-CCFA}^+} \mathbf{tr} ; \rho = \mathbf{tr} ; \rho ; \mathbf{tr}$$

Proof.

$$\begin{aligned} \mathbf{tr} ; \rho &= Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) ; \rho ; \mathbf{tr} && \text{(by Ax. 25)} \\ &= Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) ; \rho ; (\mathbf{tr} \cdot \mathbf{tr}) && \text{(by idempotence)} \\ &= Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) ; \rho ; \mathbf{tr} ; \mathbf{tr} && \text{(by Thm A.1.7)} \\ &= \mathbf{tr} ; \rho ; \mathbf{tr} && \text{(by Ax. 25)} \end{aligned}$$

■

Lemma D.5 *Let $\alpha \in ForDLTL(\Sigma)$ and $P \in PrgDLTL(\Sigma)$*

$$\vdash_{\omega\text{-CCFA}^+} \mathbf{tr};M_{DLTL}(\alpha,P) = \mathbf{tr};M_{DLTL}(\alpha,P);\mathbf{tr}$$

Proof. In order to prove the lemma, we will show that

$$\vdash_{\omega\text{-CCFA}^+} Ran\,(\mathbf{tr};M_{DLTL}(\alpha,P)) \leq \mathbf{tr} \tag{16}$$

We proceed as follows

- $P = a_i$

$$\begin{aligned}
& Ran\,(\mathbf{tr};M_{DLTL}(\alpha,a_i)) \\
&= Ran\,(\mathbf{tr};Dom\,(T_{DLTL}\,(\alpha))\,;Ran\,(\pi\nabla(\mathbf{A_i}\otimes\rho))\,;\rho) \\
&\qquad\qquad \text{(by def. } M_{DLTL}) \\
&\leq Ran\,(\mathbf{tr};\rho) && \text{(by Thm A.1.7 and monotonicity)} \\
&= Ran\,(\mathbf{tr};\rho;\mathbf{tr}) && \text{(by Lemma D.4)} \\
&= Ran\,(\mathbf{tr};\rho)\,;\mathbf{tr} && \text{(by Thm A.1.4)} \\
&\leq \mathbf{tr} && \text{(by Thm. A.2.8)}
\end{aligned}$$

- $P = R \cup S$

$$\begin{aligned}
& Ran\,(\mathbf{tr};M_{DLTL}(\alpha,R\cup S)) \\
&= Ran\,(\mathbf{tr};(M_{DLTL}(\alpha,R)+M_{DLTL}(\alpha,S))) && \text{(by def. } M_{DLTL}) \\
&= Ran\,(\mathbf{tr};M_{DLTL}(\alpha,R)+\mathbf{tr};M_{DLTL}(\alpha,S)) && \text{(by Thm A.1.13)} \\
&= Ran\,(\mathbf{tr};M_{DLTL}(\alpha,R)) + Ran\,(\mathbf{tr};M_{DLTL}(\alpha,S)) && \text{(by Thm A.1.12)} \\
&\leq \mathbf{tr}+\mathbf{tr} && \text{(by Ind. Hyp.)} \\
&= \mathbf{tr} && \text{(by idempotence)}
\end{aligned}$$

- $P = R;S$

$$\begin{aligned}
& Ran\,(\mathbf{tr};M_{DLTL}(\alpha,R;S)) \\
&= Ran\,(\mathbf{tr};M_{DLTL}(\alpha,R);M_{DLTL}(\alpha,S)) && \text{(by def. } M_{DLTL}) \\
&= Ran\,(Ran\,(\mathbf{tr};M_{DLTL}(\alpha,R))\,;M_{DLTL}(\alpha,S)) && \text{(by Thm A.1.3)} \\
&\leq Ran\,(\mathbf{tr};M_{DLTL}(\alpha,S)) && \text{(by Thm A.1.7 and Ind. Hyp.)} \\
&\leq \mathbf{tr} && \text{(by Ind. Hyp.)}
\end{aligned}$$

- $P = R^*$

$$\begin{aligned}
& Ran\,(\mathbf{tr};M_{DLTL}(\alpha,R^*)) \leq \mathbf{tr} \\
\Longleftrightarrow\; & Ran\,\left(\mathbf{tr};M_{DLTL}(\alpha,R)^*\right) \leq \mathbf{tr} && \text{(by def. } M_{DLTL}) \\
\Longleftrightarrow\; & \mathbf{tr};M_{DLTL}(\alpha,R)^* \leq \mathbf{1};\mathbf{tr} && \text{(by Thm A.1.8)} \\
\Longleftrightarrow\; & M_{DLTL}(\alpha,R)^* \leq \neg\mathbf{tr};\mathbf{1}+\mathbf{1};\mathbf{tr} && \text{(by Thm A.1.9)}
\end{aligned}$$

We will prove this using ω-rule:

– base case:

$$\begin{aligned} 1' &= \neg\mathbf{tr}+\mathbf{tr} && \text{(by Thm A.2.1)} \\ &= \neg\mathbf{tr};1'+1';\mathbf{tr} && \text{(by Ax. 5)} \\ &\le \neg\mathbf{tr};\mathbf{1}+\mathbf{1};\mathbf{tr} && \text{(by monotonicity)} \end{aligned}$$

– inductive step:

$$\begin{aligned} & M_{DLTL}(\alpha,R)^{;k+1} \\ &= M_{DLTL}(\alpha,R);M_{DLTL}(\alpha,R)^{;k} && \text{(by def. 2.33)} \\ &= \mathbf{tr};M_{DLTL}(\alpha,R);M_{DLTL}(\alpha,R)^{;k} \\ &\quad +\neg\mathbf{tr};M_{DLTL}(\alpha,R);M_{DLTL}(\alpha,R)^{;k} && \text{(by Thm A.2.9)} \\ &\le \mathbf{tr};M_{DLTL}(\alpha,R);M_{DLTL}(\alpha,R)^{;k} \\ &\quad +\neg\mathbf{tr};\mathbf{1} && \text{(by monotonicity)} \\ &= \mathbf{tr};M_{DLTL}(\alpha,R);Ran\left(\mathbf{tr};M_{DLTL}(\alpha,R)\right);M_{DLTL}(\alpha,R)^{;k} \\ &\quad +\neg\mathbf{tr};\mathbf{1} && \text{(by Thm. A.1.11)} \\ &\le \mathbf{tr};M_{DLTL}(\alpha,R);\mathbf{tr};M_{DLTL}(\alpha,R)^{;k}+\neg\mathbf{tr};\mathbf{1} \\ & && \text{(by Ind. Hyp. on } R \text{ and monotonicity)} \\ &\le \mathbf{tr};M_{DLTL}(\alpha,R);\mathbf{tr};(\neg\mathbf{tr};\mathbf{1}+\mathbf{1};\mathbf{tr})+\neg\mathbf{tr};\mathbf{1} \\ & && \text{(by Ind. Hyp. on } k \text{ and monotonicity)} \\ &= \mathbf{tr};M_{DLTL}(\alpha,R);\mathbf{tr};\neg\mathbf{tr};\mathbf{1} \\ &\quad +\mathbf{tr};M_{DLTL}(\alpha,R);\mathbf{tr};\mathbf{1};\mathbf{tr} \\ &\quad +\neg\mathbf{tr};\mathbf{1} && \text{(by Thm A.1.13)} \\ &= \mathbf{tr};M_{DLTL}(\alpha,R);\mathbf{tr}\cdot\neg\mathbf{tr};\mathbf{1} \\ &\quad +\mathbf{tr};M_{DLTL}(\alpha,R);\mathbf{tr};\mathbf{1};\mathbf{tr} \\ &\quad +\neg\mathbf{tr};\mathbf{1} && \text{(by Thm A.1.7)} \\ &\le \mathbf{tr};M_{DLTL}(\alpha,R);\mathbf{tr};\mathbf{1};\mathbf{tr}+\neg\mathbf{tr};\mathbf{1} && \text{(by Thm A.2.1)} \\ &\le \mathbf{1};\mathbf{tr}+\neg\mathbf{tr};\mathbf{1} && \text{(by monotonicity)} \end{aligned}$$

Now, we will prove both inclusions:

$\le$)

$$\mathbf{tr};M_{DLTL}(\alpha,P);\mathbf{tr} \le \mathbf{tr};M_{DLTL}(\alpha,P) \qquad \text{(by Thm. A.2.8)}$$

$\ge$)

$$\begin{aligned} \mathbf{tr};M_{DLTL}(\alpha,P) &= \mathbf{tr};M_{DLTL}(\alpha,P);Ran\left(\mathbf{tr};M_{DLTL}(\alpha,P)\right) \\ & && \text{(by Thm. A.1.11)} \\ &\le \mathbf{tr};M_{DLTL}(\alpha,P);\mathbf{tr} && \text{(by (16) and monotonicity)} \end{aligned}$$

Lemma D.6

$$\vdash_{\omega\text{-CCFA}^+} \mathbf{tr} = \mathbf{tr} ; Ran\,(\pi \nabla (\mathbf{T} \otimes \rho))$$

Proof. We begin by proving that

$$\neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) \cdot \mathbf{tr} = 0 \tag{17}$$

$$\begin{aligned}
&\neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) \cdot \mathbf{tr} \\
&= \neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) \cdot \mathbf{tr} \cdot \mathbf{tr} && \text{(by idempotence)} \\
&= \neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) ; \mathbf{tr} ; \mathbf{tr} && \text{(by Thm. A.1.7)} \\
&\leq \neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) ; \mathbf{tr} ; (\mathbf{S} \otimes \mathbf{tr}) && \text{(by Ax. 24)} \\
&= \neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) ; \mathbf{tr} ; (\pi ; \mathbf{S} \nabla \rho ; \mathbf{tr}) && \text{(by def. } \otimes) \\
&= \begin{pmatrix} \neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) ; \mathbf{tr} ; \pi ; \mathbf{S} \\ \nabla \\ \neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) ; \mathbf{tr} ; \rho ; \mathbf{tr} \end{pmatrix} && \text{(by Thm. A.4.4)} \\
&= \begin{pmatrix} \neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) ; \mathbf{tr} ; \pi ; \mathbf{S} \\ \nabla \\ \neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) ; Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) ; \rho ; \mathbf{tr} ; \mathbf{tr} \end{pmatrix} && \text{(by Ax. 25)} \\
&= \begin{pmatrix} \neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) ; \mathbf{tr} ; \pi ; \mathbf{S} \\ \nabla \\ (\neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) \cdot Ran\,(\pi \nabla (\mathbf{T} \otimes \rho))) ; \rho ; \mathbf{tr} ; \mathbf{tr} \end{pmatrix} && \text{(by Thm. A.1.7)} \\
&= \begin{pmatrix} \neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) ; \mathbf{tr} ; \pi ; \mathbf{S} \\ \nabla \\ 0 \end{pmatrix} && \text{(by Thm. A.1.1 and Thm. A.2.2)} \\
&= (\neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) ; \mathbf{tr} ; \pi ; \mathbf{S} ; \breve{\pi}) \cdot (0 ; \breve{\rho}) && \text{(by Ax. 8)} \\
&= 0 && \text{(by Thm. A.1.1 and BA)}
\end{aligned}$$

Therefore,

$$\begin{aligned}
\mathbf{tr} &= \mathbf{tr} ; Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) + \mathbf{tr} ; \neg Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) && \text{(by Thm. A.2.9)} \\
&= \mathbf{tr} ; Ran\,(\pi \nabla (\mathbf{T} \otimes \rho)) && \text{(by (17))}
\end{aligned}$$

■

Lemma D.7 *Let* $\alpha \in ForDLTL(\Sigma)$ *and* $A = \{a_i\}_{i \in \mathcal{P}}$.

$$\vdash_{\omega\text{-CCFA}^+} \mathbf{tr} ; M_{DLTL}(\alpha, \bigcup_{i \in \mathcal{P}} a_i) = \mathbf{tr} ; Dom\,(T_{DLTL}\,(\alpha)) ; \rho$$

Proof.

$$\mathbf{tr}; M_{DLTL}(\alpha, \bigcup_{i \in \mathcal{P}} a_i)$$

$$\begin{aligned}
&= \mathbf{tr}; (+_{i \in \mathcal{P}} Dom\,(T_{DLTL}\,(\alpha))\,; Ran\,(\pi \nabla (\mathbf{A_i} \otimes \rho))\,; \rho) && \text{(by def. } M_{DLTL}\text{)} \\
&= \mathbf{tr}; Dom\,(T_{DLTL}\,(\alpha))\,; (+_{i \in \mathcal{P}} Ran\,(\pi \nabla (\mathbf{A_i} \otimes \rho))\,; \rho && \text{(by Lemma A.1.13)} \\
&= \mathbf{tr}; Dom\,(T_{DLTL}\,(\alpha))\,; Ran\,(+_{i \in \mathcal{P}} (\pi \nabla (\mathbf{A_i} \otimes \rho)))\,; \rho && \text{(by Thm. A.1.12)} \\
&= \mathbf{tr}; Dom\,(T_{DLTL}\,(\alpha))\,; Ran\,(\pi \nabla (+_{i \in \mathcal{P}} \mathbf{A_i} \otimes \rho))\,; \rho && \text{(by Thm. A.4.11)} \\
&= \mathbf{tr}; Dom\,(T_{DLTL}\,(\alpha))\,; Ran\,(\pi \nabla (\mathbf{T} \otimes \rho))\,; \rho && \text{(by Ax. 26)} \\
&= \mathbf{tr}; Dom\,(T_{DLTL}\,(\alpha))\,; \mathbf{tr}; Ran\,(\pi \nabla (\mathbf{T} \otimes \rho))\,; \rho && \text{(by Thms. A.2.7 and A.2.5)} \\
&= \mathbf{tr}; Dom\,(T_{DLTL}\,(\alpha))\,; \mathbf{tr}; \rho && \text{(by lemma D.6)} \\
&= \mathbf{tr}; Dom\,(T_{DLTL}\,(\alpha))\,; \rho && \text{(by Thms. A.2.7 and A.2.5)}
\end{aligned}$$

■

Lemma D.8 *Let* $\Sigma = \langle A, P \rangle$ *be a signature. Let* $\alpha \in ForLTL(P)$

$$\vdash_{\omega\text{-CCFA}^+} \mathbf{tr}; T_{LTL}(\alpha) = \mathbf{tr}; T_{DLTL}\,(T_{LTL \to DLTL}(\alpha))$$

Proof. We will prove this lemma by induction on the complexity of formula α.

- $\alpha = p_i$

$$\begin{aligned}
\mathbf{tr}; T_{LTL}(p_i) &= \mathbf{tr}; \pi; \mathbf{P_i} && \text{(by def. } T_{LTL}(\alpha)\text{)} \\
&= \mathbf{tr}; T_{DLTL}\,(p_i) && \text{(by def. } T_{DLTL}\text{)} \\
&= \mathbf{tr}; T_{DLTL}\,(T_{LTL \to DLTL}(p_i)) && \text{(by def. } T_{LTL \to DLTL}\text{)}
\end{aligned}$$

- $\alpha = \neg\beta$.
  In order to prove the equality we will use Lemma A.1.6. We will begin by proving that the hypothesis of Lemma A.1.6 are satisfied. First, it is easy to see that,

$$\begin{aligned}
\mathbf{tr}; T_{LTL}(\beta) \cdot \mathbf{tr}; \overline{T_{LTL}(\beta)} &= \mathbf{tr}; (T_{LTL}(\beta) \cdot \overline{T_{LTL}(\beta)}) && \text{(by Thm. A.1.17)} \\
&= \mathbf{tr}; 0 && \text{(BA)} \\
&= 0 && \text{(by Thm. A.1.1)}
\end{aligned}$$

  Then,

$$\mathbf{tr}; T_{LTL}(\beta) \cdot \mathbf{tr}; \overline{T_{LTL}(\beta)} = 0 \tag{18}$$

  The proof for

$$\mathbf{tr}; T_{DLTL}\,(T_{LTL \to DLTL}(\beta)) \cdot \mathbf{tr}; \overline{T_{DLTL}\,(T_{LTL \to DLTL}(\beta))} = 0 \tag{19}$$

  follows in a similar way. We also have that,

$$\mathbf{tr}; T_{LTL}(\beta) = \mathbf{tr}; T_{DLTL}\,(T_{LTL \to DLTL}(\beta)) \quad \text{(by Ind. Hyp.)} \tag{20}$$

Also,

$$\mathbf{tr};T_{LTL}(\beta)+\mathbf{tr};\overline{T_{LTL}(\beta)} = \mathbf{tr};(T_{LTL}(\beta)+\overline{T_{LTL}(\beta)}) \quad \text{(by Lemma A.1.13)}$$
$$= \mathbf{tr};\mathbf{1} \quad \text{(BA)}$$

Then,

$$\mathbf{tr};T_{LTL}(\beta)+\mathbf{tr};\overline{T_{LTL}(\beta)} = \mathbf{tr};\mathbf{1} \tag{21}$$

The proof for

$$\mathbf{tr};T_{DLTL}\,(T_{LTL\to DLTL}(\beta)) + \mathbf{tr};\overline{T_{DLTL}\,(T_{LTL\to DLTL}(\beta))} = \mathbf{tr};\mathbf{1} \tag{22}$$

follows in a similar way.
Then, as the hypothesis that of Lemma A.1.6 are valid, we proceed as follows.
Joining (18)-(22), by Lemma A.1.6,

$$\mathbf{tr};\overline{T_{LTL}(\beta)} = \mathbf{tr};\overline{T_{DLTL}\,(T_{LTL\to DLTL}(\beta))} \tag{23}$$

Therefore,

$$\begin{aligned}
\mathbf{tr};T_{LTL}(\neg\beta) &= \mathbf{tr};\mathbf{tr};\overline{T_{LTL}(\beta)} && \text{(by def. } T_{LTL}\text{)}\\
&= \mathbf{tr};\mathbf{tr};\overline{T_{DLTL}\,(T_{LTL\to DLTL}(\beta))} && \text{(by (23))}\\
&= \mathbf{tr};T_{DLTL}\,(\neg T_{LTL\to DLTL}(\beta)) && \text{(by def. } T_{DLTL}\text{)}\\
&= \mathbf{tr};T_{DLTL}\,(T_{LTL\to DLTL}(\neg\beta)) && \text{(by def. } T_{LTL\to DLTL}\text{)}
\end{aligned}$$

- $\alpha = \beta \vee \gamma$

$$\begin{aligned}
&\mathbf{tr};T_{LTL}(\beta\vee\gamma)\\
&= \mathbf{tr};(T_{LTL}(\beta)+T_{LTL}(\gamma)) && \text{(by def. } T_{LTL}(\alpha)\text{)}\\
&= \mathbf{tr};T_{LTL}(\beta)+\mathbf{tr};T_{LTL}(\gamma) && \text{(by Lemma A.1.13)}\\
&= \mathbf{tr};T_{DLTL}\,(T_{LTL\to DLTL}(\beta)) + \mathbf{tr};T_{DLTL}\,(T_{LTL\to DLTL}(\gamma)) && \text{(by Ind. Hyp.)}\\
&= \mathbf{tr};(T_{DLTL}\,(T_{LTL\to DLTL}(\beta)) + T_{DLTL}\,(T_{LTL\to DLTL}(\gamma))) && \text{(by Lemma A.1.13)}\\
&= \mathbf{tr};T_{DLTL}\,(T_{LTL\to DLTL}(\beta)\vee T_{LTL\to DLTL}(\gamma)) && \text{(by def. } T_{DLTL}\text{)}\\
&= \mathbf{tr};T_{DLTL}\,(T_{LTL\to DLTL}(\beta\vee\gamma)) && \text{(by def. } T_{LTL\to DLTL}\text{)}
\end{aligned}$$

- $\alpha = \oplus\beta$

$$\begin{aligned}
\mathbf{tr};T_{LTL}(\oplus\beta) &= \mathbf{tr};\rho;T_{LTL}(\beta) && \text{(by def. } T_{LTL}\text{)}\\
&= \mathbf{tr};\rho;\mathbf{tr};T_{LTL}(\beta) && \text{(by Lemma D.4)}\\
&= \mathbf{tr};\rho;\mathbf{tr};T_{DLTL}\left(T_{LTL\to DLTL}(\beta)\right) && \text{(by Ind. Hyp.)}\\
&= \mathbf{tr};\rho;T_{DLTL}\left(T_{LTL\to DLTL}(\beta)\right) && \text{(by Lemma D.4)}\\
&= \mathit{Dom}\left(\mathbf{tr};T_{DLTL}\left(\mathbf{true}\right)\right);\rho;T_{DLTL}\left(T_{LTL\to DLTL}(\beta)\right)\\
& && \text{(by Lemma D.3)}\\
&= \mathbf{tr};\mathit{Dom}\left(T_{DLTL}\left(\mathbf{true}\right)\right);\rho;T_{DLTL}\left(T_{LTL\to DLTL}(\beta)\right)\\
& && \text{(by Lemma A.1.4)}\\
&= \mathbf{tr};M_{DLTL}(\mathbf{true},\bigcup_{i\in\mathcal{P}} a_i);T_{DLTL}\left(T_{LTL\to DLTL}(\beta)\right)\\
& && \text{(by Lemma D.7)}\\
&= \mathbf{tr};T_{DLTL}\left(\mathbf{true}\ \mathsf{U}^{\bigcup_{i\in\mathcal{P}} a_i}\ T_{LTL\to DLTL}(\beta)\right)\\
& && \text{(by def. } T_{DLTL}\text{)}\\
&= \mathbf{tr};T_{DLTL}\left(T_{LTL\to DLTL}(\oplus\beta)\right) && \text{(by def. } T_{LTL\to DLTL}\text{)}
\end{aligned}$$

- $\alpha = \beta\ \mathsf{U}\ \gamma$

$$\begin{aligned}
&\mathbf{tr};T_{LTL}(\beta\ \mathsf{U}\ \gamma)\\
&= \mathbf{tr};\left(\mathit{Dom}\left(T_{LTL}(\beta)\right);\rho\right)^*;T_{LTL}(\gamma) && \text{(by def. } T_{LTL}\text{)}\\
&= \mathbf{tr};\left(\mathbf{tr};\mathit{Dom}\left(T_{LTL}(\beta)\right);\rho;\mathbf{tr}\right)^*;T_{LTL}(\gamma) && \text{(by Lemma A.3)}\\
&= \mathbf{tr};\left(\mathit{Dom}\left(T_{LTL}(\beta)\right);\mathbf{tr};\rho;\mathbf{tr}\right)^*;T_{LTL}(\gamma) && \text{(by Thm. A.2.5)}\\
&= \mathbf{tr};\left(\mathit{Dom}\left(T_{LTL}(\beta)\right);\mathbf{tr};\rho\right)^*;T_{LTL}(\gamma) && \text{(by Lemma D.4)}\\
&= \mathbf{tr};\left(\mathbf{tr};\mathit{Dom}\left(T_{LTL}(\beta)\right);\rho\right)^*;T_{LTL}(\gamma) && \text{(by Thm. A.2.5)}\\
&= \mathbf{tr};\left(\mathit{Dom}\left(\mathbf{tr};T_{LTL}(\beta)\right);\rho\right)^*;T_{LTL}(\gamma) && \text{(by Lemma A.1.4)}\\
&= \mathbf{tr};\left(\mathit{Dom}\left(\mathbf{tr};T_{DLTL}\left(T_{LTL\to DLTL}(\beta)\right)\right);\rho\right)^*;T_{LTL}(\gamma)\\
& && \text{(by Ind. Hyp.)}\\
&= \mathbf{tr};\left(\mathbf{tr};\mathit{Dom}\left(T_{DLTL}\left(T_{LTL\to DLTL}(\beta)\right)\right);\rho\right)^*;T_{LTL}(\gamma)\\
& && \text{(by Lemma A.1.4)}\\
&= \mathbf{tr};\left(\mathbf{tr};M_{DLTL}(T_{LTL\to DLTL}(\beta),\bigcup_{i\in\mathcal{P}} a_i)\right)^*;T_{LTL}(\gamma)\\
& && \text{(by Lemma D.7)}\\
&= \mathbf{tr};M_{DLTL}(T_{LTL\to DLTL}(\beta),\bigcup_{i\in\mathcal{P}} a_i)^*;T_{LTL}(\gamma) && \text{(by Lemma A.3)}\\
&= \mathbf{tr};M_{DLTL}(T_{LTL\to DLTL}(\beta),(\bigcup_{i\in\mathcal{P}} a_i)^*);T_{LTL}(\gamma) && \text{(by def. } M_{DLTL}\text{)}
\end{aligned}$$

$$= \mathbf{tr};M_{DLTL}(T_{LTL\to DLTL}(\beta),(\bigcup_{i\in\mathcal{P}} a_i)^*);T_{DLTL}\,(T_{LTL\to DLTL}(\gamma))$$

(by Ind. Hyp.)

$$= \mathbf{tr};T_{DLTL}\left(T_{LTL\to DLTL}(\beta)\ \mathsf{U}^{(\bigcup_{i\in\mathcal{P}} a_i)^*}\ T_{LTL\to DLTL}(\gamma)\right)$$

(by def. T_{DLTL})

$$= \mathbf{tr};T_{DLTL}\,(T_{LTL\to DLTL}(\beta\ \mathsf{U}\ \gamma)) \qquad \text{(by def. } T_{LTL\to DLTL})$$

■

Lemma D.9 *Let $\Sigma = \langle A, P\rangle$ be a signature. Let $\alpha \in ForProp(P)$. Then,*

$$\vdash_{\omega\text{-CCFA+}} \mathbf{tr};\pi;T_{PDL}(\alpha) = \mathbf{tr};T_{LTL}(\alpha)$$

Proof. It follows by induction on the complexity of formula α .

- $\alpha = p_i$

$$\begin{aligned}\mathbf{tr};\pi;T_{PDL}(p_i) &= \mathbf{tr};\pi;\mathbf{P_i} && \text{(by def. } T_{PDL}(\alpha))\\ &= \mathbf{tr};T_{LTL}(p_i) && \text{(by def. } T_{LTL}(\alpha))\end{aligned}$$

- $\alpha = \beta \vee \gamma$

$$\begin{aligned}\mathbf{tr};\pi;T_{PDL}(\beta\vee\gamma) &= \mathbf{tr};\pi;(T_{PDL}(\beta)+T_{PDL}(\gamma)) && \text{(by def. } T_{PDL}(\alpha))\\ &= \mathbf{tr};\pi;T_{PDL}(\beta)+\mathbf{tr};\pi;T_{PDL}(\gamma) && \text{(by Lemma A.1.13)}\\ &= \mathbf{tr};T_{LTL}(\beta)+\mathbf{tr};T_{LTL}(\gamma) && \text{(by Ind. Hyp.)}\\ &= \mathbf{tr};(T_{LTL}(\beta)+T_{LTL}(\gamma)) && \text{(by Lemma A.1.13)}\\ &= \mathbf{tr};T_{LTL}(\beta\vee\gamma) && \text{(by def. } T_{LTL}(\alpha))\end{aligned}$$

- $\alpha = \neg\beta$
  First, note that

$$\begin{aligned}Ran\,(\mathbf{tr};\pi) &= ((\mathbf{tr};\pi)^{\smile};(\mathbf{tr};\pi))\cdot 1' && \text{(by def. } Ran)\\ &= (\breve{\pi};\breve{\mathbf{tr}};\mathbf{tr};\pi)\cdot 1' && \text{(by Ax. 6)}\\ &= (\breve{\pi};\mathbf{tr};\mathbf{tr};\pi)\cdot 1' && \text{(by Thm. A.1.6)}\\ &= (\breve{\pi};\mathbf{tr};\pi)\cdot 1' && \text{(by Thm. A.2.7)}\\ &= \mathbf{S}\cdot 1' && \text{(by Ax. 23)}\\ &= \mathbf{S} && \text{(by Ax. 16)}\end{aligned}$$

  Then,

$$Ran\,(\mathbf{tr};\pi) = \mathbf{S} \tag{24}$$

Now, we continue by proving that hypothesis of Lemma A.1.7 are satisfied.

$$\begin{aligned}
\mathbf{tr};\pi;T_{PDL}(\alpha)+\mathbf{tr};\pi;\overline{T_{PDL}(\alpha)} &= \mathbf{tr};\pi;(T_{PDL}(\alpha)+\overline{T_{PDL}(\alpha)}) \\
&\qquad \text{(by Lemma A.1.13)} \\
&= \mathbf{tr};\pi;\mathbf{1} \qquad \text{(BA)} \\
&= \mathbf{tr};\mathbf{1} \qquad \text{(by Lemma A.1.11)}
\end{aligned}$$

and,

$$\begin{aligned}
\mathbf{tr};T_{LTL}(\alpha)+\mathbf{tr};\overline{T_{LTL}(\alpha)} &= \mathbf{tr};(T_{LTL}(\alpha)+\overline{T_{LTL}(\alpha)}) \\
&\qquad \text{(by Lemma A.1.13)} \\
&= \mathbf{tr};\mathbf{1} \qquad \text{(BA)}
\end{aligned}$$

It follows that,

$$\mathbf{tr};\pi;T_{PDL}(\alpha)+\mathbf{tr};\pi;\overline{T_{PDL}(\alpha)} = \mathbf{tr};T_{LTL}(\alpha)+\mathbf{tr};\overline{T_{LTL}(\alpha)} \tag{25}$$

On the other hand, by Ind. Hyp.

$$\mathbf{tr};\pi;T_{PDL}(\alpha) = \mathbf{tr};T_{LTL}(\alpha) \tag{26}$$

Also,

$$\begin{aligned}
(\mathbf{tr};\pi;T_{PDL}(\alpha))\cdot(\mathbf{tr};\pi;\overline{T_{PDL}(\alpha)}) &= \mathbf{tr};\pi;(T_{PDL}(\alpha)\cdot\overline{T_{PDL}(\alpha)}) \\
&\qquad \text{(by Thm. A.1.17)} \\
&= \mathbf{tr};\pi;0 \qquad \text{(BA)} \\
&= 0 \qquad \text{(by Thm. A.1.1)}
\end{aligned}$$

Then,

$$(\mathbf{tr};\pi;T_{PDL}(\alpha))\cdot(\mathbf{tr};\pi;\overline{T_{PDL}(\alpha)}) = 0 \tag{27}$$

The proof for

$$(\mathbf{tr};T_{LTL}(\alpha))\cdot(\mathbf{tr};\overline{T_{LTL}(\alpha)}) = 0 \tag{28}$$

follows in a similar way.
Thus, joining (25)-(28) and by Lemma A.1.7

$$\mathbf{tr};\pi;\overline{T_{PDL}(\alpha)} = \mathbf{tr};\overline{T_{LTL}(\alpha)} \tag{29}$$

Finally, we have that,

$$\begin{aligned}
\mathbf{tr};\pi;T_{PDL}(\neg\beta) &= \mathbf{tr};\pi;\mathbf{S};\overline{T_{PDL}(\beta)} && \text{(by def. } T_{PDL}(\alpha)\text{)} \\
&= \mathbf{tr};\pi;\overline{T_{PDL}(\beta)} && \text{(by (24))} \\
&= \mathbf{tr};\overline{T_{LTL}(\beta)} && \text{(by (29))} \\
&= \mathbf{tr};\mathbf{tr};\overline{T_{LTL}(\beta)} && \text{(by Thm. A.2.7)} \\
&= \mathbf{tr};T_{LTL}(\neg\beta) && \text{(by def. } T_{LTL}(\alpha)\text{)}
\end{aligned}$$

■

Lemma D.10

$$\vdash_{\omega\text{-CCFA}^+} \mathbf{tr}_{\mathbf{0}}^{\rightarrow} = \mathbf{tr}_{\mathbf{0}}^{\rightarrow} ; \mathbf{tr}$$

Proof. In order to prove the lemma, we will show that

$$\vdash_{\omega\text{-CCFA}^+} \mathbf{tr}_{\mathbf{0}}^{\rightarrow} \leq \mathbf{tr} \tag{30}$$

We proceed as follows

$$\begin{aligned}
\mathbf{tr}_{\mathbf{0}}^{\rightarrow} &= Ran\,(\mathbf{tr}_{\mathbf{0}} ; \rho^*) && \text{(by def. } \mathbf{tr}_{\mathbf{0}}^{\rightarrow}) \\
&= Ran\,(Dom\,(\pi ; \mathbf{S}_{\mathbf{0}}) ; \mathbf{tr} ; \rho^*) && \text{(by def. } \mathbf{tr}_{\mathbf{0}}) \\
&\leq Ran\,(\mathbf{tr} ; \rho^*) && \text{(by Thm. A.2.8)} \\
&= Ran\,(\mathbf{tr} ; \rho^* ; \mathbf{tr}) && \text{(by Lemma A.3)} \\
&= Ran\,(\mathbf{tr} ; \rho^*) ; \mathbf{tr} && \text{(by Lemma A.1.4)} \\
&\leq \mathbf{tr} && \text{(by Thm. A.2.8)}
\end{aligned}$$

Now, we prove both inclusions

$\leq$)

$$\begin{aligned}
\mathbf{tr}_{\mathbf{0}}^{\rightarrow} &= \mathbf{tr}_{\mathbf{0}}^{\rightarrow} ; \mathbf{tr}_{\mathbf{0}}^{\rightarrow} && \text{(by Thm. A.2.7)} \\
&\leq \mathbf{tr}_{\mathbf{0}}^{\rightarrow} ; \mathbf{tr} && \text{(by (30) and monotonicity)}
\end{aligned}$$

$\geq$)

$$\mathbf{tr}_{\mathbf{0}}^{\rightarrow} ; \mathbf{tr} \leq \mathbf{tr}_{\mathbf{0}}^{\rightarrow} \qquad \text{(by Thm. A.2.8)}$$

■

Lemma D.11

$$\vdash_{\omega\text{-CCFA}^+} \mathbf{tr}_{\mathbf{0}}^{\rightarrow} ; \rho = \mathbf{tr}_{\mathbf{0}}^{\rightarrow} ; \rho ; \mathbf{tr}_{\mathbf{0}}^{\rightarrow}$$

Proof. In order to prove the lemma, we will show that

$$\vdash_{\omega\text{-CCFA}^+} Ran\,(\mathbf{tr}_{\mathbf{0}}^{\rightarrow} ; \rho) \leq \mathbf{tr}_{\mathbf{0}}^{\rightarrow} \tag{31}$$

$$\begin{aligned}
Ran\,(\mathbf{tr}_{\mathbf{0}}^{\rightarrow} ; \rho) &= Ran\,(Ran\,(\mathbf{tr}_{\mathbf{0}} ; \rho^*) ; \rho) && \text{(by def. } \mathbf{tr}_{\mathbf{0}}^{\rightarrow}) \\
&= Ran\,(\mathbf{tr}_{\mathbf{0}} ; \rho^* ; \rho) && \text{(by Lemma A.1.3)} \\
&\leq Ran\,(\mathbf{tr}_{\mathbf{0}} ; \rho^*) && \text{(by } \rho^* ; \rho \leq \rho^* \text{ and monotonicity of } Ran) \\
&= \mathbf{tr}_{\mathbf{0}}^{\rightarrow} && \text{(by def. } \mathbf{tr}_{\mathbf{0}}^{\rightarrow})
\end{aligned}$$

Now, we prove both inclusions

≤)

$$\begin{aligned} \mathbf{tr}_\mathbf{0}^{\rightarrow};\rho &= \mathbf{tr}_\mathbf{0}^{\rightarrow};\rho;Ran(\mathbf{tr}_\mathbf{0}^{\rightarrow};\rho) && \text{(by Thm. A.1.11)}\\ &\leq \mathbf{tr}_\mathbf{0}^{\rightarrow};\rho;\mathbf{tr}_\mathbf{0}^{\rightarrow} && \text{(by (31) and monotonicity)} \end{aligned}$$

≥)

$$\mathbf{tr}_\mathbf{0}^{\rightarrow};\rho;\mathbf{tr}_\mathbf{0}^{\rightarrow} \leq \mathbf{tr}_\mathbf{0}^{\rightarrow};\rho \qquad \text{(by Thm. A.2.8)}$$

■

Lemma D.12

$$\vdash_{\omega\text{-CCFA}^+} \mathbf{S};\mathbf{A_i} = \mathbf{A_i}$$

Proof.
≤)

$$\mathbf{S};\mathbf{A_i} \leq \mathbf{A_i} \qquad \text{(by Thm. A.2.8)}$$

≥)

$$\begin{aligned} \mathbf{A_i} &= \mathbf{S};\mathbf{A_i};\mathbf{S} && \text{(by Ax. 19)}\\ &\leq \mathbf{S};\mathbf{A_i} && \text{(by Thm. A.2.8)} \end{aligned}$$

■

Lemma D.13

$$\vdash_{\omega\text{-CCFA}^+} \mathbf{A_i};\mathbf{S} = \mathbf{A_i}$$

Proof. The proof is analogous to Lemma D.12. ■

Lemma D.14

$$\vdash_{\omega\text{-CCFA}^+} Dom(\mathbf{A_i}) = Dom(\mathbf{A_i});\mathbf{S}$$

Proof.

$$\begin{aligned} Dom(\mathbf{A_i}) &= Dom(\mathbf{S};\mathbf{A_i}) && \text{(by Lemma D.12)}\\ &= \mathbf{S};Dom(\mathbf{A_i}) && \text{(by Lemma A.1.4)}\\ &= Dom(\mathbf{A_i});\mathbf{S} && \text{(by Thm. A.2.5)} \end{aligned}$$

■

Lemma D.15

$$\vdash_{\omega\text{-CCFA}^+} \mathbf{tr_0} = \mathbf{tr_0};\mathbf{tr}$$

Proof.

$$\begin{aligned} \mathbf{tr_0} &= Ran(\pi;\mathbf{S_0});\mathbf{tr} && \text{(by def. } \mathbf{tr_0})\\ &= Ran(\pi;\mathbf{S_0});\mathbf{tr};\mathbf{tr} && \text{(by Thm. A.2.7)}\\ &= \mathbf{tr_0};\mathbf{tr} && \text{(by def. } \mathbf{tr_0}) \end{aligned}$$

■

E Reasoning across formalisms: Semantic approach

In this appendix we present a proof for Thm. 6.1.

Lemma E.1 *Let K be a Kripke structure that is a model for the theory $DLTL(\Sigma)$. Let $\alpha \in ForProp(P)$, and $s \in \Delta_K$.*

$$(\forall j)(K^{LTL}, s^j \models_{LTL} \alpha \Longleftrightarrow K^{PDL}, s_j \models_{PDL} \alpha)$$

Proof. It follows by induction on the formula structure. ■

Lemma E.2 *Let $K = \langle S, \tilde{A}, \tilde{P} \rangle$ be a Kripke structure that is a model for the theory $PDL(\Sigma)$, let $\alpha, \beta \in ForPDL(\Sigma)$, let $a \in A$, and let $p, q \in S$. Then,*

$$(K, p \models_{PDL} \alpha \wedge K, p \models_{PDL} \alpha \Longrightarrow [a]\beta \wedge \langle p, q \rangle \in \tilde{a}) \Longrightarrow K, q \models_{PDL} \beta$$

Proof.

$$\begin{aligned}
& K, p \models_{PDL} \alpha \wedge K, p \models_{PDL} \alpha \Longrightarrow [a]\beta \wedge \langle p, q \rangle \in \tilde{a} \\
\Longrightarrow & K, p \models_{PDL} \alpha \wedge (K, p \not\models_{PDL} \alpha \vee K, p \models_{PDL} [a]\beta) \wedge \langle p, q \rangle \in \tilde{a} \\
\Longrightarrow & K, p \models_{PDL} [a]\beta \wedge \langle p, q \rangle \in \tilde{a} \\
\Longrightarrow & K, p \models_{PDL} \neg\langle a \rangle \neg\beta \wedge \langle p, q \rangle \in \tilde{a} \\
\Longrightarrow & K, p \not\models_{PDL} \langle a \rangle \neg\beta \wedge \langle p, q \rangle \in \tilde{a} && \text{(by def. of } \models_{PDL}) \\
\Longrightarrow & \neg(\exists p')(K, p' \models_{PDL} \neg\beta \wedge \langle p, p' \rangle \in \tilde{a}) \wedge \langle p, q \rangle \in \tilde{a} && \text{(by def. of } \models_{PDL}) \\
\Longrightarrow & \neg(\exists p')(K, p' \not\models_{PDL} \beta \wedge \langle p, p' \rangle \in \tilde{a}) \wedge \langle p, q \rangle \in \tilde{a} && \text{(by def. of } \models_{PDL}) \\
\Longrightarrow & K, q \models_{PDL} \beta
\end{aligned}$$

■

Lemma E.3 *Let $K = \langle S, T, S_0, \tilde{P} \rangle$ a Kripke structure that is a model for the theory $LTL(P)$, let $\alpha, \beta, \gamma \in ForLTL(P)$, and let $s \in \Delta_K$. If,*

$$\begin{aligned}
& K, s \models_{LTL} \alpha \text{ and,} \\
& K, s \models_{LTL} \beta \text{ and,} \\
& K, s^1 \models_{LTL} \gamma \text{ and,} \\
& K, s \models_{LTL} (\alpha \wedge \beta) \Longrightarrow \oplus(\gamma \Longrightarrow \beta)
\end{aligned}$$

then,

$$K, s^1 \models_{LTL} \beta$$

Proof.

$$K, s \models_{LTL} \alpha$$
$$\wedge\, K, s \models_{LTL} \beta$$
$$\wedge\, K, s^1 \models_{LTL} \gamma$$
$$\wedge\, K, s \models_{LTL} (\alpha \wedge \beta) \Longrightarrow \oplus(\gamma \Longrightarrow \beta)$$
$$\Longrightarrow$$
$$K, s \models_{LTL} \alpha \wedge \beta$$
$$\wedge\, K, s^1 \models_{LTL} \gamma$$
$$\wedge\, K, s \models_{LTL} (\alpha \wedge \beta) \Longrightarrow \oplus(\gamma \Longrightarrow \beta) \qquad \text{(by def. of } \models_{LTL}\text{)}$$
$$\Longleftrightarrow$$
$$K, s \models_{LTL} \alpha \wedge \beta$$
$$\wedge\, K, s^1 \models_{LTL} \gamma$$
$$\wedge\, ((K, s \not\models_{LTL} \alpha \wedge \beta) \vee (K, s \models_{LTL} \oplus(\gamma \Longrightarrow \beta))) \qquad \text{(by def. of } \models_{LTL}\text{)}$$
$$\Longleftrightarrow$$
$$K, s \models_{LTL} \alpha \wedge \beta$$
$$\wedge\, K, s^1 \models_{LTL} \gamma$$
$$\wedge\, K, s \models_{LTL} \oplus(\gamma \Longrightarrow \beta)$$
$$\Longleftrightarrow$$
$$K, s \models_{LTL} \alpha \wedge \beta$$
$$\wedge\, K, s^1 \models_{LTL} \gamma$$
$$\wedge\, K, s^1 \models_{LTL} \gamma \Longrightarrow \beta \qquad \text{(by def. of } \models_{LTL}\text{)}$$
$$\Longrightarrow$$
$$K, s^1 \models_{LTL} \beta \qquad \text{(by def. of } \models_{LTL}\text{)}$$

■

Lemma E.4 *Given K a Kripke structure that is a model for the theory $DLTL(\Sigma)$ and satisfies Thm. 6.1 hypothesis. Let $s \in \Delta_K$ and $P \in PrgDLTL(\Sigma)$.*

$$(\forall k)(exec(s,k) \in \|P\|_K \Longrightarrow ((K, s \not\models_{DLTL} I') \vee (\forall j \in [0,k])(K, s^j \models_{DLTL} I')))$$

Proof. Let us assume k such that $exec(s,k) \in \|P\|_K$. The proof follows by induction on the structure of program P.

- $P = a_i$

– If $K^{LTL}, s \not\models_{LTL} I$ we prove it as follows,

$$
\begin{aligned}
& K^{LTL}, s \not\models_{LTL} I \\
\Longrightarrow & K, s \not\models_{DLTL} T_{LTL\to DLTL}(I) && \text{(by Thm. 5.1)} \\
\Longrightarrow & K, s \not\models_{DLTL} I' && \text{(by def. of } I'\text{)} \\
\Longrightarrow & (K, s \not\models_{DLTL} I') \vee (\forall j \in [0,k])(K, s^j \models_{DLTL} I')
\end{aligned}
$$

– If $K^{LTL}, s \models_{LTL} I$, we proceed as follows.
Since K satisfies Thm. 6.1 hypothesis, we have that,

$$
\begin{aligned}
& K^{PDL}, s_0 \models_{PDL} \alpha_i \Longrightarrow [a_i]\beta_i, \\
& K^{PDL}, s_0 \models_{PDL} \neg\alpha_i \Longrightarrow [a_i]\textbf{false}, \text{ and,} \\
& K^{LTL}, s \models_{LTL} (\alpha_i \wedge I) \Longrightarrow \oplus(\beta_i \Longrightarrow I)
\end{aligned}
$$

And since $exec(s,k) \in \|a_i\|_K$, we can conclude that,

$$
\begin{aligned}
& K^{PDL}, s_0 \models_{PDL} \alpha_i \Longrightarrow [a_i]\beta_i \\
& \wedge K^{PDL}, s_0 \models_{PDL} \neg\alpha_i \Longrightarrow [a_i]\textbf{false} \\
& \wedge K^{LTL}, s \models_{LTL} (\alpha_i \wedge I) \Longrightarrow \oplus(\beta_i \Longrightarrow I) \\
& \wedge K^{LTL}, s \models_{LTL} I \\
& \wedge exec(s,k) \in \|a_i\|_K \\
\Longleftrightarrow & \\
& K^{PDL}, s_0 \models_{PDL} \alpha_i \Longrightarrow [a_i]\beta_i \\
& \wedge K^{PDL}, s_0 \models_{PDL} \neg\alpha_i \Longrightarrow [a_i]\textbf{false} \\
& \wedge K^{LTL}, s \models_{LTL} (\alpha_i \wedge I) \Longrightarrow \oplus(\beta_i \Longrightarrow I) \\
& \wedge K^{LTL}, s \models_{LTL} I \\
& \wedge \langle s_0, s_1 \rangle \in \tilde{a}_i \\
& \wedge k = 1 && \text{(by def. 5.6)} \\
\Longleftrightarrow & \\
& K^{PDL}, s_0 \models_{PDL} \alpha_i \Longrightarrow [a_i]\beta_i \\
& \wedge (K^{PDL}, s_0 \models_{PDL} \alpha_i \vee \neg(\exists s')\, \langle s_0, s' \rangle \in \tilde{a}_i) \\
& \wedge K^{LTL}, s \models_{LTL} (\alpha_i \wedge I) \Longrightarrow \oplus(\beta_i \Longrightarrow I) \\
& \wedge K^{LTL}, s \models_{LTL} I \\
& \wedge \langle s_0, s_1 \rangle \in \tilde{a}_i \\
& \wedge k = 1 && \text{(by def. of } \models_{PDL}\text{)}
\end{aligned}
$$

$$\Longrightarrow$$

$$K^{PDL}, s_0 \models_{PDL} \alpha_i \Longrightarrow [a_i]\beta_i$$
$$\wedge\, K^{LTL}, s \models_{LTL} (\alpha_i \wedge I) \Longrightarrow \oplus(\beta_i \Longrightarrow I)$$
$$\wedge\, K^{LTL}, s \models_{LTL} I$$
$$\wedge\, \langle s_0, s_1\rangle \in \tilde{a_i}$$
$$\wedge\, k = 1$$
$$\wedge\, K^{PDL}, s_0 \models_{PDL} \alpha_i$$

$$\Longrightarrow K^{LTL}, s \models_{LTL} (\alpha_i \wedge I) \Longrightarrow \oplus(\beta_i \Longrightarrow I)$$
$$\wedge\, K^{LTL}, s \models_{LTL} I$$
$$\wedge\, k = 1$$
$$\wedge\, K^{PDL}, s_0 \models_{PDL} \alpha_i$$
$$\wedge\, K^{PDL}, s_1 \models_{PDL} \beta_i \qquad \text{(by Lemma E.2)}$$

$$\Longrightarrow$$

$$K^{LTL}, s \models_{LTL} (\alpha_i \wedge I) \Longrightarrow \oplus(\beta_i \Longrightarrow I)$$
$$\wedge\, K^{LTL}, s \models_{LTL} I$$
$$\wedge\, k = 1$$
$$\wedge\, K^{LTL}, s \models_{LTL} \alpha_i$$
$$\wedge\, K^{LTL}, s^1 \models_{LTL} \beta_i \qquad \text{(by Lemma E.1)}$$

$$\Longrightarrow$$

$$K^{LTL}, s \models_{LTL} I$$
$$\wedge\, K^{LTL}, s^1 \models_{LTL} I$$
$$\wedge\, k = 1 \qquad \text{(by Lemma E.3)}$$

$$\Longrightarrow$$

$$K, s \models_{DLTL} I'$$
$$\wedge\, K, s^1 \models_{DLTL} I'$$
$$\wedge\, k = 1 \qquad \text{(by Lemma 5.1)}$$
$$\Longrightarrow (\forall j \in [0,k])(K, s^j \models_{DLTL} I')$$
$$\Longrightarrow (K, s \not\models_{DLTL} I') \vee (\forall j \in [0,k])(K, s^j \models_{DLTL} I')$$

- $P = R \cup S$

$$exec(s,k) \in \|R \cup S\|_K$$
$$\Longrightarrow exec(s,k) \in \|R\|_K \cup \|S\|_K \qquad \text{(by def. 5.6)}$$
$$\Longrightarrow exec(s,k) \in \|R\|_K \vee exec(s,k) \in \|S\|_K \qquad \text{(by set theory)}$$
$$\Longrightarrow K, s \not\models_{DLTL} I' \;\vee (\forall j \in [0,k])(K, s^j \models_{DLTL} I') \qquad \text{(by Ind. Hyp.)}$$

- $P = R; S$

$$
\begin{aligned}
& exec(s,k) \in \|R;S\|_K \\
\Longrightarrow & exec(s,k) \in \|R\|_K ; \|S\|_K && \text{(by def. 5.6)} \\
\Longrightarrow & (\exists \tau)(\exists \tau')((exec(s,k) = \tau;\tau') \wedge (\tau \in \|R\|_K) \wedge (\tau' \in \|S\|_K)) \\
& && \text{(by def. 5.4)}
\end{aligned}
$$

  - If it is the case that $\tau = \lambda$:

$$
\begin{aligned}
\Longrightarrow & \lambda \in \|R\|_K \wedge exec(s,k) \in \|S\|_K \\
\Longrightarrow & \lambda \in \|R\|_K \wedge (K, s \not\models_{DLTL} I' \vee (\forall j \in [0,k])(K, s^j \models_{DLTL} I')) \\
& && \text{(by Ind. Hyp.)} \\
\Longrightarrow & K, s \not\models_{DLTL} I' \vee (\forall j \in [0,k])(K, s^j \models_{DLTL} I')
\end{aligned}
$$

  - The proof for the case that $\tau' = \lambda$ is analogous to the previous one.
  - If it is the case that $\tau \neq \lambda$ and $\tau' \neq \lambda$ is true:

$$\Longrightarrow \quad (\exists k' \in (0,k))((exec(s,k') \in \|R\|_K) \wedge (exec(s^{k'}, k-k') \in \|S\|_K))$$

by Ind. Hyp.

$$
\Longrightarrow \quad
\begin{aligned}
& (\exists k' \in (0,k))(\\
& (K, s \not\models_{DLTL} I' \vee (\forall j \in [0,k'])(K, s^j \models_{DLTL} I')) \wedge \\
& (K, s^{k'} \not\models_{DLTL} I' \vee (\forall j \in [0,k-k'])(K, (s^{k'})^j \models_{DLTL} I')))
\end{aligned}
$$

$$
\Longrightarrow \quad
\begin{aligned}
& (\exists k' \in (0,k))(\\
& (\underbrace{K, s \not\models_{DLTL} I'}_{a} \vee \underbrace{(\forall j \in [0,k'])(K, s^j \models_{DLTL} I')}_{b}) \wedge \\
& (\underbrace{K, s^{k'} \not\models_{DLTL} I'}_{c} \vee \underbrace{(\forall j \in [k',k])(K, s^j \models_{DLTL} I')}_{d}))
\end{aligned}
$$

It is easy to see that $b \Longrightarrow \neg c$.
So from $(a \vee b) \wedge (c \vee d)$ we can conclude that $a \vee (c \wedge d)$

$$
\Longrightarrow \quad
\begin{aligned}
& (\exists k' \in (0,k))((K, s \not\models_{DLTL} I') \vee \\
& (\forall j \in [k,k'])(K, s^j \models_{DLTL} I') \wedge (\forall j \in [k',k])(K, s^j \models_{DLTL} I'))
\end{aligned}
$$

$$\Longrightarrow \quad (K, s \not\models_{DLTL} I') \vee (\forall j \in [0,k])(K, s^j \models_{DLTL} I')$$

- $P = R^*$

$$
\begin{aligned}
& exec(s,k) \in \|R^*\|_K \\
\Longrightarrow & exec(s,k) \in (\|R\|_K)^* && \text{(by def. 5.6)} \\
\Longrightarrow & (\exists n \in [0,\infty))(exec(s,k) \in \|R\|^{;n}) && \text{(by def. of *)}
\end{aligned}
$$

We will prove that

$$\begin{array}{l}(\exists n \in [0,\infty))(\\ \quad (exec(s,k) \in (\|R\|_K)^{;n}) \\ \qquad \Longrightarrow ((K, s \not\models_{DLTL} I') \vee (\forall j \in [0,k])(K, s^j \models_{DLTL} I')))\end{array}$$

by induction on natural n.

- base case

$$\begin{aligned} & exec(s,k) \in (\|R\|_K)^{;0} \\ \Longrightarrow & exec(s,k) \in \{\lambda\} && \text{(by def. 5.6)} \\ \Longrightarrow & exec(s,k) = \lambda && \text{(by set theory)} \\ \Longrightarrow & k = 0 && \text{(by def. of } exec\text{)} \\ \Longrightarrow & (K, s \not\models_{DLTL} I') \vee (\forall j \in [0,k])(K, s^j \models_{DLTL} I') \end{aligned}$$

- inductive step

$$\begin{aligned} & exec(s,k) \in (\|R\|_K)^{;n+1} \\ \Longrightarrow & exec(s,k) \in \|R\|_K ; (\|R\|_K)^{;n} && \text{(by def. 5.6)} \end{aligned}$$

The rest of the proof is analogous to the $P = R; S$ case.

■

Lemma E.5 *Given K a Kripke structure that is a model for the theory $DLTL(\Sigma)$ satisfying Thm. 6.1 hypothesis. Let $s \in \Delta_K$ and $P \in PrgDLTL(\Sigma)$.*

$$(\exists k \in [0,\infty))(exec(s,k) \in \|P\|_K) \Longrightarrow K, s \models_{DLTL} I' \Longrightarrow (I' \, \mathsf{U}^P \, I')$$

Proof.

$$
\begin{aligned}
&(\exists k \in [0,\infty))(exec(s,k) \in \|P\|_K) \\
\Longrightarrow &(\exists k \in [0,\infty))((K,s \not\models_{DLTL} I') \vee (\forall j \in [0,k])(K,s^j \models_{DLTL} I')) \\
& \hfill \text{(by Lemma E.4)} \\
\Longrightarrow &(\exists k \in [0,\infty))(\\
&\quad (K,s \not\models_{DLTL} I') \vee \\
&\quad ((\forall j \in [0,k])(K,s^j \models_{DLTL} I') \wedge (exec(s,k) \in \|P\|_K))) \\
\Longleftrightarrow &(\exists k \in [0,\infty))(\\
&\quad (K,s \not\models_{DLTL} I') \vee \\
&\quad (K,s^k \models_{DLTL} I') \wedge \\
&\quad (\forall j \in [0,k))(K,s^j \models_{DLTL} I') \wedge \\
&\quad (exec(s,k) \in \|P\|_K))) \\
\Longleftrightarrow &(K,s \not\models_{DLTL} I') \vee \\
&\quad (\exists k \geq 0)(\\
&\quad (K,s^k \models_{DLTL} I') \wedge \\
&\quad (\forall j \in [0,k))(K,s^j \models_{DLTL} I') \wedge \\
&\quad (exec(s,k) \in \|P\|_K))) \\
\Longleftrightarrow &(K,s \not\models_{DLTL} I') \vee (K,s \models_{DLTL} I' \,\mathsf{U}^P\, I') && \text{(by def. of } \models_{DLTL}) \\
\Longleftrightarrow &K,s \models_{DLTL} I' \Longrightarrow (I' \,\mathsf{U}^P\, I') && \text{(by def. of } \models_{DLTL})
\end{aligned}
$$

■

Lemma E.6 *Given K a Kripke structure that is a model for the theory $DLTL(\Sigma)$ satisfying Thm. 6.1 hypothesis. Let $s \in \Delta_K$ and $P \in PrgDLTL(\Sigma)$.*

$$K,s \models_{DLTL} \mathbf{true}\,\mathsf{U}^P\,\mathbf{true} \Longrightarrow (I' \Longrightarrow (I' \,\mathsf{U}^P\, I'))$$

Proof.

$$
\begin{aligned}
&K,s \models_{DLTL} \mathbf{true}\,\mathsf{U}^P\,\mathbf{true} \\
\Longleftrightarrow &(\exists k \in [0,\infty))(exec(s,k) \in \|P\|_K) && \text{(by Lemma C.3)} \\
\Longrightarrow &(\exists k \in [0,\infty))(K,s \models_{DLTL} I' \Longrightarrow (I' \,\mathsf{U}^P\, I')) && \text{(by Lemma E.5)} \\
\Longleftrightarrow &K,s \models_{DLTL} I' \Longrightarrow (I' \,\mathsf{U}^P\, I')
\end{aligned}
$$

Then,

$$K,s \models_{DLTL} \mathbf{true}\,\mathsf{U}^P\,\mathbf{true} \Longrightarrow (I' \Longrightarrow (I' \,\mathsf{U}^P\, I'))$$

■

Theorem E.1 *Let K be a Kripke structure that is a model for the theory $DLTL(\Sigma)$, such that*

- K^{PDL} *is a model of specPDL.*
- K^{LTL} *is a model of specLTL.*

Then, K is a model of specDLTL.

Proof. The proof is almost trivial from the previous results. Given K a Kripke structure for logic $DLTL(\Sigma)$ satisfying Thm. 6.1 hypothesis, then by Lemma E.5 it follows that every axiom of *specDLTL* is valid in K. Therefore, K is a model of *specDLTL*. ■