INFORMATIQUE THÉORIQUE ET APPLICATIONS

A. MASINI
A. MAGGIOLO-SCHETTINI

TTL : a formalism to describe local and global properties of distributed systems

Informatique théorique et applications, tome 26, n° 2 (1992), p. 115-149.

<http://www.numdam.org/item?id=ITA_1992__26_2_115_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 26, n° 2, 1992, p. 115 à 149)

TTL: A FORMALISM TO DESCRIBE LOCAL AND GLOBAL PROPERTIES OF DISTRIBUTED SYSTEMS (*)

by A. MASINI (1) and A. MAGGIOLO-SCHETTINI (1)

Abstract. – *In this paper we develop a logic formalism to describe and prove properties of finite-state distributed systems. This formalism is based on a branching time approach and is called Typed Temporal Logic* (**TTL**). *For a distributed system* D, *we give two* **TTL** *theories,* $\mathbf{LTT}_D$ *and* $\mathbf{LGTT}_D$ (*Local Time Theory and Local and Global Time Theory of D, respectively*). *The theory* $\mathbf{LTT}_D$ *allows specifying distributed systems by local axioms, namely by properties that hold with respect to local observations of system parts. The theory* $\mathbf{LGTT}_D$ *has a mechanism to infer global properties of the system D from local properties. For both the theories we show that theorem proving is reducible to model checking.*

Résumé. – *Dans ce travail on développe un formalisme logique qui permet de formuler et de prouver des propriétés de systèmes répartis à états finis. Ce formalisme se base sur la notion de « branching time » et s'appelle Typed Temporal Logic* (**TTL**). *Pour un système réparti D on introduit deux théories de* **TTL**, c'est-à-dire $\mathbf{LTT}_D$ *et* $\mathbf{LGTT}_D$ (*Local Time Theory et Local and Global Time Theory of D, respectivement*). *La théorie* $\mathbf{LTT}_D$ *permet de spécifier des systèmes répartis par des axiomes locaux, c'est-à-dire propriétés qui sont vraies par rapport à des observations locales de parties de systèmes. La théorie* $\mathbf{LTT}_D$ *possède un mécanisme pour déduire des propriétés globales du système D à partir de propriétés locales. Pour les deux théories on prouve que la notion de démontrabilité est réductible à la notion de vérité dans un modèle.*

INTRODUCTION

In the last 10 years a number of temporal logics has been proposed with the aim of modeling and specifying concurrent and distributed systems (*see* e. g. Ben-Ari, Pnueli and Manna [2], Clarke, Grumberg and Kurshan [4], Kröger [15], Manna and Wolper [18], Nguyen, Demers, Gries and Owicki [20]).

Using temporal logics seems to be quite natural if one wants to describe behaviors which are strictly time dependent. In particular, branching time logics are preferable when one needs to deal with alternative computation

(*) Received September 1990, accepted November 1990.
Research partially supported by C.N.R. Progetto Finalizzato Informatica e Calcolo Parallelo and by C.N.R. Gruppo Nazionale Informatica Matematica.
(1) Dipartimento di Informatica, Università di Pisa, Corso Italia 40, 56100 Pisa, Italy.

Informatique théorique et Applications/Theoretical Informatics and Applications
0988-3754/92/02 115 35/$5.50/

paths (*see* Ben-Ari, Pnueli and Manna [2], Danelutto and Masini [6], Emerson [8], Emerson and Clarke [9], Emerson and Halpern [11], Emerson and Lei [12], Lamport [16]).

Moreover, it has been observed that considering a system as a whole and the time expressed by the alternation of system global configurations is not very satisfactory when reasoning on distributed systems (*see* Degano, De Nicola and Montanari [7] for an approach based on rewriting systems, and Clarke, Long and McMillan [5], Enjalbert and Michel [14], Lodaya and Thiagarajan [17] for a temporal logic approach).

We can think of a distributed system as composed of a finite set of interacting parts, where each part is partially independent from the others and the only dependences between parts are given by interactions. This concept of a distributed system naturally leads to considering each part as having a local time. As a consequence of this point of view, we introduce a pure typed temporal logic (**TTL**) and, by using **TTL**, for any distributed system D, we develop a theory $\mathbf{LTT}_D$ (Local Time Theory of D), where each type is related to the time of a part of the considered distributed system. For each type a visibility function specifies which informations are accessible to the correspondent part for its advancement. In $\mathbf{LTT}_D$ we define the concept of local state, which consists of the inner state of a part p plus portions of the inner states of the other parts which are visible by p. The theory $\mathbf{LTT}_D$ has a set of local well formed formulas, called unitary local formulas, as axioms. Such axioms specify, for each local state, the set of possible next time local states (with respect to local times). In this way distributed systems are formalized only by local properties (local axioms) that the single parts must enjoy, without any global assumption.

In order to prove global properties of the whole system D, we define another theory of **TTL** called $\mathbf{LGTT}_D$ (Local and Global Time Theory of D) that is a conservative extension of $\mathbf{LTT}_D$. The theory $\mathbf{LGTT}_D$ has a new type related to the global time of the system. In a way similar to the one followed for $\mathbf{LTT}_D$, the concepts of global states and unitary global formulas are defined (unitary global formulas specify, for each global state, the possible next time global states). The idea of $\mathbf{LGTT}_D$ is that unitary global formulas are obtained from unitary local formulas. To this aim $\mathbf{LGTT}_D$ is equipped with a set of multityped inference rules,

In order to show that $\mathbf{LTT}_D$ and $\mathbf{LGTT}_D$ are good formalizations of distributed systems with respect to provability of properties, we define two finite models, $\mathscr{H}_D$ for $\mathbf{LTT}_D$ and $\mathscr{H}_D^+$ for $\mathbf{LGTT}_D$. Provability in the theories $\mathbf{LTT}_D$ and $\mathbf{LGTT}_D$ is shown to be reducible to model checking in $\mathscr{H}_D$ and

$\mathscr{H}_D^+$, respectively. As model checking in $\mathscr{H}_D$ and $\mathscr{H}_D^+$ can be done in $\mathscr{P}$-time (*see* Danelutto and Masini [6]) we have $\mathscr{P}$-time decision algorithms for provability in $\mathbf{LTT}_D$ and $\mathbf{LGTT}_D$. (As regards temporal model checking and decision problem *see* e. g. Ben-Ari, Pnueli and Manna [2], Clarke, Emerson and Sistla [3], Clarke, Grumberg and Kurshan [4], Clarke, Long and McMillan [5], Danelutto and Masini [6], Emerson and Halpern [10], Emerson and Lei [12], Emerson and Sistla [13]).

An early version of the theory $\mathbf{LTT}_D$ has been defined in Masini [19].

The paper is organized as follows: in section 1 we give the concepts of distributed system, visibility and decomposition; in section 2 we define the formal system **TTL** giving its syntax and its semantics; in section 3 we give the theory $\mathbf{LTT}_D$; in section 4 we give the theory $\mathbf{LGTT}_D$; in appendix we prove some model properties for $\mathbf{LTT}_D$ and $\mathbf{LGTT}_D$.

1. DISTRIBUTED SYSTEMS

In this section we introduce a concept of distributed system inspired by Wedde's Interaction Systems (*see* [21]). Our intuition is that a distributed system consists of a finite set of spatially distributed parts which may interact. There is no centralized control. Each part consists of a finite set of activity phases, and, at a certain time, a part may be in one and one only of its phases, called *current phase*. A part passes from one phase to another following an internal program, and compatibly with interactions with other parts. More precisely, a *distributed system* (or briefly a *system*) is a quintuple $D = \langle A, P, B, M, R \rangle$, where:

$A = \{a_1, \ldots, a_m\}$ is a finite nonempty set of activity phases (briefly *phases*),

$P = \{p_1, \ldots, p_n\}$ is a partition of A with each p called *part*,

$B = \{b_{p_1}, \ldots, b_{p_n}\}$ is such that each b_p is a directed graph $\langle p, \rightarrow \rangle$ where $\rightarrow \subseteq p \times p - \mathrm{id}(p)$ and for each $a \in p$ there exists $a' \neq a$ s. t. $a \rightarrow a'$; this graph (or *program*) gives the allowed *internal behavior* of the part, such that if a is the *current phase* of part p and p *leaves* a, then p may *enter* only a phase a' with $a \rightarrow a'$ being an arc of the graph,

$M \subseteq A^2 - \mathrm{id}(A)$ is a symmetric relation between phases such that $\forall p \in P$ $(p^2 - \mathrm{id}(p)) \subseteq M$ and if $a \in p$ and $a' \in p'$ with $(a, a') \in M$ a cannot be current phase of p if a' is current phase of p', and symmetrically, and moreover if $a, a' \in M$, $a \in p$, $a' \in p'$, $p \neq p'$, a is the current phase of p whereas a' is not the current phase of p', then p' cannot enter a' while p has not left a (*mutual exclusion*),

$R \subseteq A^2 - \bigcup_{p \in P} p^2$, is a symmetric relation between phases such that for $a \in p$, $a' \in p'$ and $(a, a') \in R$: (i) if a, a' are current phases of p and p', respectively, p leaves a iff p' leaves a', (ii) if a is the current phase of p then p cannot leave phase a until p' has not entered phase a' and symmetrically (*synchronization relation*).

The synchronization relation considered here corresponds to a synchronous "send/receive". Excluding arcs $a \to a$ from behaviours of parts is due to the fact that we want that a change of phase corresponds to each arc of the graph.

We shall call $\mathscr{D}$ the class of Distributed Systems.

1.1. *Example:* In the figure 1 we show a graphic representation of a distributed system. Single pointed arrows give programs of parts. Undirected arcs between phases give the relation M, double undirected arcs between phases give the relation R. Mutual exclusions between phases of the same part are not shown. ■

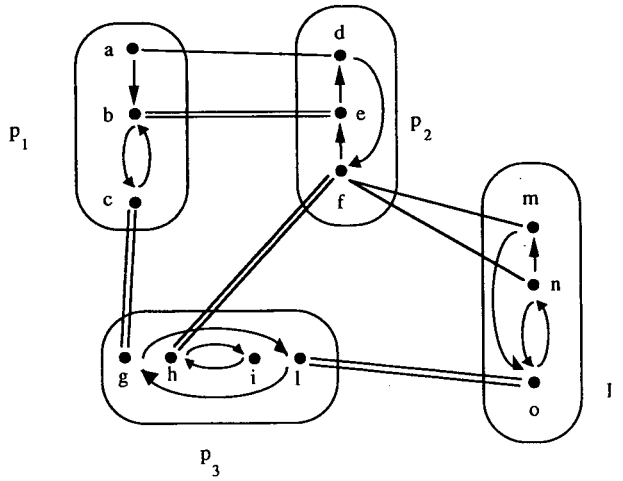


Figure 1.

As a distributed system is supposed to be without a centralized control, each part must have no knowledge of other parts but for what is needed for possible interactions.

We introduce now the concepts of visibility and decompositions. Given a system D, for each phase a of a part p of D the visibility function gives the

set of parts which have knowledge of a, in the sense that such parts know whether part p is currently in phase a or not.

1.2. DEFINITION (*Visibility*): For $D=\langle A, P, B, M, R\rangle \in \mathscr{D}$, the function $V_D: A \to 2^P$ such that, for $p \in P$ and $a \in A$, $p \in V_D(a)$ iff either

(i) $a \in p$

or

(ii) $\exists a'(a, a') \in R \cup M$ and $a' \in p$

is called *visibility function*. ■

In V_D we shall omit the subscript D when the considered system is clear from the context.

1.3. *Example:* For the system in figure 1 we have: $V(f)=\{p_2, p_3, p_4\}$ as phase f belongs to p_2 and is in a relation (M or R) with the parts p_3 and p_4, $V(i)=\{p_3\}$ as phase i is in no relation with phases of other parts. ■

A decomposition of a system D with respect to a part p of D gives a system consisting of p itself together with portions of other parts p' containing phases a such that $p \in V(a)$ plus "slack phases" $*_{p'}$, namely phases that stand for all possible phases $a \in p'$ such that $p \notin V(a')$. As we do not want that a part has knowledge of programs of the interacting parts, we assume that in the decomposition of D for $p \neq p'$ the behaviours allow all the possible transitions between phases (but the ones from phases to themselves).

1.4. DEFINITION (*Decomposition*): For $D=\langle A, P, B, M, R\rangle \in \mathscr{D}$, we call *decomposition of* D the function $\mathrm{Dec}_D: P \to \mathscr{D}$ such that, for $p \in P$, $\mathrm{Dec}_D(p)=\langle A', P', B', M', R'\rangle$ with:

$$P'=\{p\} \cup \{\tilde{p}': p' \in P-\{p\} \wedge \tilde{p}'=\{a': a' \in p' \wedge p \in V(a')\} \cup \{*_{p'}\}\},$$

$$A'=\bigcup_{p' \in P'} p',$$

$$M'=\bigcup_{p' \in P'} (p'^2\text{-id}(p')) \cup \{(a_1, a_2): (a_1, a_2) \in M, a_1 \in p\},$$

$$R'=\{(a_1, a_2): (a_1, a_2) \in R, a_1 \in p\},$$

$$B'=\{b_p\} \cup \{b': b'=\langle p', p'^2\text{-id}(p)\rangle \text{ and } p' \in P'-\{p\}\}$$

where $*_p$ denotes the slack phase of part p.

The system $\mathrm{Dec}_D(p)$ is called *subsystem* of D. Given a part p and

$$\mathrm{Dec}_D(p)=\langle A', P', B', M', R'\rangle$$

with $\mathrm{Dec}_D(p)$. A we denote A', with $\mathrm{Dec}_D(p)$. P we denote P', etc. In Dec_D we shall omit the subscript D when the considered system is clear from the context. ■

1.5. *Example:* Let us consider the system of figure 1. Figure 2 shows the subsystem $\mathrm{Dec}(p_1)$. ■

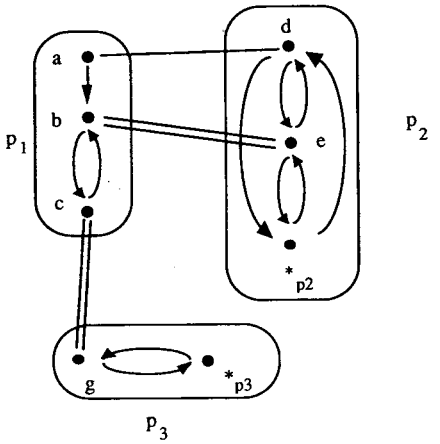


Figure 2

1.6. DEFINITION: Given $D=\langle A, P, B, M, R\rangle$, a subset $S\subseteq A$ is called a *global configuration* of D iff

1. $\forall a, a' \in S\ (a, a') \notin M$,
2. $\forall p \in P \mid p \cap S \mid = 1$.

If D is a subsystem of D', namely D belongs to the image of $\mathrm{Dec}_{D'}$, the global configurations of D are called *local configurations.* ■

1.7. *Example:* The sets $\{a, e, m, i\}$, $\{b, f, o, l\}$ are global configurations of the system in figure 1, whereas $\{b, f, o\}$ is not a global configration as it does not contain any phase of part p_3. ■

2. THE SYSTEM TTL

In this section we introduce a typed pure logic called Typed Temporal Logic (**TTL**). The idea of **TTL** is that of giving a typization of propositional symbols plus an observation function in order to build and derive typed well formed formulas.

We assume the knowledge of some branching time logic. For its simplicity we use the Unified system of Branching time (*UB*) described by Ben-Ari, Pnueli and Manna in [2] (*see* also Emerson and Sistla [13]).

The language of *UB* contains the usual propositional connectives $\supset$, $\wedge$, $\vee$, $\neg$, and temporal quantifiers *AX*, *EX*, *AG*, *EG*, *AF*, *EF*. The time is assumed to be discrete. If α is a formula of *UB*, we have the following informal meanings of temporal quantifiers: $AX\alpha$ stands for "α is true in each next time", $EX\alpha$ for "α is true in some next time", $AG\alpha$ for "α is true in each state of every possible future", $EG\alpha$ for "α is true in each state of some possible future", $AF\alpha$ for "α is true in some state of every possible future", $EF\alpha$ for "α is true in some state of some possible future".

2.1. Syntax of TTL

Well formed formulas (wff)

Given $\mathrm{TYP} = \{t_1, \ldots, t_n\}$, a set of types, $\mathrm{PROP} = \{a_1, \ldots, a_n\}$, a set of propositional symbols, $\neg$, $\supset$, connectives, *EX*, *EF*, *EG*, temporal quantifiers, $O : \mathrm{PROP} \to 2^{\mathrm{TYP}}$, an *observation function*, for each type t the set of well formed formulas (wff) of type t or wff_t is defined as follows:

$\alpha \in \mathrm{wff}_t \Leftrightarrow$

(i) $\alpha \in \mathrm{PROP}$, $t \in O(\alpha)$ (α is said to be an *atomic* wff_t)

or

(ii) $\alpha \in \{\neg\beta, \beta \supset \gamma, EX\beta, EF\beta, EG\beta \mid \beta, \gamma \in \mathrm{wff}_t\}$.

We shall use the following abbreviations:

$\alpha \wedge \beta$ for $\neg(\alpha \supset \neg\beta)$, $\alpha \vee \beta$ for $\neg\alpha \supset \beta$, $AX\alpha$ for $\neg EX \neg\alpha$, $AF\alpha$ for $\neg EG \neg\alpha$, $AG\alpha$ for $\neg EF \neg\alpha$.

Logical axioms and inference rules

For each type t all *UB* axioms and inference rules are *logical axioms and inference rules of type t.*

For example if $t \in \mathrm{TYP}$, $\alpha, \beta \in \mathrm{wff}_t$, then $AG(\alpha \supset \beta) \supset (AG\alpha \supset AG\beta)$ is a logical axiom of type t.

Mathematical axioms

For each type t it is possible to add to **TTL** a set Ψ_t of wff_t as axioms, called *mathematical axioms of type t.*

Each $\Psi = \{\Psi_{t_1}, \ldots, \Psi_{t_n}\}$ defines a *theory* of **TTL** with Ψ as set of mathematical axioms.

A theory of **TTL** without mathematical axioms is called a *pure calculus* of **TTL**.

TTL theorems

If $\Psi = \{\Psi_{t_1}, \ldots, \Psi_{t_n}\}$ and $t \in \{t_1, \ldots, t_n\}$, we shall write $\Psi \underset{t}{\vdash} \alpha$ to mean that α is a wff of type t and a syntactic consequence of the formulas in Ψ_t. If Ψ is empty (*i.e.* each Ψ_t is empty) α is called *theorem w.r.t. type t* of **TTL**. If T is a theory of **TTL** with Ψ as a set of mathematical axioms we shall use also the notation $T \underset{t}{\vdash} \alpha$ as equivalent to $\Psi \underset{t}{\vdash} \alpha$; in this case we say that α is a *theorem w.r.t. type t* of the theory T. ■

It is important to point out that t in the notation $\underset{t}{\vdash}$ cannot be omitted. Actually, as we shall see in the next section, it will be possible to have two different types t' and t'', an n-tuple $\Psi = \{\Psi_{t_1}, \ldots, \Psi_{t_n}\}$ of (consistent) mathematical axioms and a wff α (of type t' and type t'') s.t. $\Psi \underset{t'}{\vdash} \alpha$ and $\Psi \underset{t''}{\nvdash} \alpha$ (possibly also $\Psi \underset{t'}{\vdash} \neg\alpha$).

2.2. Semantics of TTL

We call *interpretation* for **TTL** the n-tuple:

$$\mathcal{M} = \langle \mathcal{M}_{t_1}, \ldots, \mathcal{M}_{t_n} \rangle$$

where for $t \in \{t_1, \ldots, t_n\}$, $\mathcal{M}_t = \langle W_t, N_t, P_t \rangle$ with:

W_t a denumerable set whose elements are called *worlds* of type t,

$N_t \subseteqq W_t^2$ a *successor relation* of type t,

P_t a function mapping the worlds of W_t into sets of propositional symbols of type t, *i.e.* $P_t : W_t \to 2^{\mathrm{PROP}_t}$ where $\mathrm{PROP}_t = \{\alpha : t \in O(\alpha)\}$.
For each $w \in W_t$, the sequence $f_w = \{w_j\}_{j<\omega}$ with $w_0 = w$, $\forall j \geqq 0$ $(w_j, w_{j+1}) \in N_t$ is said to be a *w-path* of type t.

Each $\mathcal{M}_t$, called a *t-subinterpretation* of $\mathcal{M}$, defines an interpretation for the sublogic of **TTL** obtained by considering only wff ot type t, ■

2.3. DEFINITION: Let $\mathcal{M} = \langle \mathcal{M}_{t_1}, \ldots, \mathcal{M}_{t_n} \rangle$ be an interpretation, t be a type, $M_t = \langle W_t, N_t, P_t \rangle$, $w \in W_t$ and α a wff of type t. We say that α is *true w.r.t.*

type t at w in $\mathcal{M}$, and we write $\mathcal{M}, w \underset{t}{\models} \alpha$, iff:

α is atomic and $\alpha \in P_t(w)$

or $\alpha \equiv \neg\beta$ and not $\mathcal{M}, w \underset{t}{\models} \beta$

or $\alpha = \beta \supset \gamma$ and $\mathcal{M}, w \underset{t}{\models} \beta \Rightarrow \mathcal{M}, w \underset{t}{\models} \gamma$

or $\alpha = EX\beta$ and $\exists w' (N_t(w, w')$ and $\mathcal{M}, w' \underset{t}{\models} \beta)$

or $\alpha = EG\beta$ and $\exists f_w \forall w' (w' \in f_w \Rightarrow \mathcal{M}, w' \underset{t}{\models} \beta)$

or $\alpha = EF\beta$ and $\exists f_w \exists w' (w' \in f_w$ and $\mathcal{M}, w' \underset{t}{\models} \beta$. Given a theory T of **TTL** an interpretation $\mathcal{M}$ is a *model* iff for each $t \in TYP$ and $\alpha \in \text{wff}_t$ $T \underset{t}{\vdash} \alpha \Rightarrow \forall w \in W_t \mathcal{M}, w \underset{t}{\models} \alpha$. ■

We shall write $\mathcal{M}, w' \underset{t}{\not\models} \alpha$ instead of not $\mathcal{M}, w' \underset{t}{\models} \alpha$.

2.4. DEFINITION: Let $t \in TYP$ and $\alpha \in \text{wff}_t$, α is said to be:

satisfiable w.r.t. type t if there is an interpretation $\mathcal{M}$ and a world $w \in W_t$ s. t. $\mathcal{M}, W \underset{t}{\models} \alpha$,

true w.r.t. type t in an interpretation $\mathcal{M}$ if $\forall w \in W_t \mathcal{M}$, $W \underset{t}{\models} \alpha$ (we shall write $\mathcal{M} \underset{t}{\models} \alpha$),

false w.r.t. type t in an interpretation $\mathcal{M}$ if $\forall w \in W_t \mathcal{M}$, $W \underset{t}{\not\models} \alpha$ (we shall write $\mathcal{M} \underset{t}{\not\models} \alpha$),

valid w.r.t. type t if α is true w.r.t. type t in each model $\mathcal{M}$ (we shall write $\underset{t}{\models} \alpha$),

contradictory w.r.t. type t if α is false w.r.t. type t in each model $\mathcal{M}$. ■

Each interpretation $\mathcal{M}$ is a model of the pure calculus **TTL** as each t-subinterpretation $\mathcal{M}_t$ of $\mathcal{M}$ is a model of *UB* (*see* Ben-Ari, Pnueli and Manna [2]).

Note that it is possible to have $\mathcal{M} \underset{t}{\models} \alpha$ and $\mathcal{M} \underset{t'}{\models} \neg\alpha$ for $t \neq t'$ (an example of this will be seen in 3.20).

3. THEORIES OF TTL FOR DISTRIBUTED SYSTEMS WITH LOCAL TIMES

In the following we are interested to use **TTL** to formalize distributed systems. To this aim, for each distributed system $D \in \mathcal{D}$ we add a (finite) set Ψ_D of suitable mathematical axioms to the pure calculus **TTL**. We shall call $\mathbf{LTT}_D$ (Local Time Theory of D) the resulting theory, which represents the **TTL** formalization of the system D.

In order to obtain $\mathbf{LTT}_D$ we must first give the **TTL** syntax for the system D, namely we must give a specific set of types and propositional symbols plus a specific observation function.

3.1. Syntax of $\mathbf{LTT}_D$

Given $D = \langle A, P, B, M, R \rangle \in \mathcal{D}$, the syntax of $\mathbf{LTT}_D$ is the one given in 2.1 for **TTL** with a specific set of types $TYP = \{ t_p : p \in P \}$, a set of propositional symbols $\text{PROP} = \bigcup_{p \in P} \text{Dec}(p).A$, and an observation function O_L such that:

$$O_L(a) = V(a) \qquad \text{for} \quad a \in A$$

$$O_L(*_p) = \{ p' : p' \in P,\ p \neq p',\ *_p \in \text{Dec}(p').A \} \qquad \text{for} \quad *_p \in \text{PROP-}A,$$

where V is the visibility function of 1.2. ■

We can observe that to each part p of D we associate a type t_p and consequently a set of well formed formulas wff_{t_p}. Such formulas express properties of the subsystem $\text{Dec}(p)$, namely properties which are local properties of the system D.

3.2. Example: Let us consider the system D of example 1.1. To each part we associate a type, namely $\text{TYP} = \{ t_{p_1}, t_{p_2}, t_{p_3}, t_{p_4} \}$. For each type $t \in \text{TYP}$ we have a rule to build the set wff_t; for example the following ones are wff of type t_{p_1}:

$$\alpha = AG \neg (a \wedge d), \beta = b \wedge e \supset AX(\neg b \equiv \neg e) \quad \text{and} \quad \gamma = AG(*_{p_2} \wedge c \wedge g)$$

as for each propositional symbol x in α, β, γ we have that $t_{p_1} \in O_L(x)$. The formula $c \wedge f \supset EX b$ is not a wff of type t_{p_1} because $t_{p_1} \notin O_L(f)$. ■

The rest of this section is devoted to give a proof system to establish which of the wff_{t_p} are theorems w.r.t. type t, *i.e.* which of the local properties given by wff_{t_p} are really enjoyed by the subsystem $\text{Dec}(p)$. We start with giving a formalization of the concept of local configuration.

3.3. DEFINITION: Given $D \in \mathcal{D}$, for $p \in P$, let $\{a_{i_1}, \ldots, a_{i_k}\}$ be a local configuration of Dec (p); the $\text{wff}_{t_p}\ a_{i_1} \wedge \ldots \wedge a_{i_k}$ is called *local state* (of type t_p). With LS_{t_p} we denote the set of local states of type t_p. ■

Given a local state $S = a_{i_1} \wedge \ldots \wedge a_{i_k}$, with abuse of notation we shall write $a \in S$ $(a \notin S)$ to say that $a \in \{a_{i_1}, \ldots, a_{i_k}\}$ $(a \notin \{a_{i_1}, \ldots, a_{i_k}\})$.

In order to completely formalize local configurations we state properties of local states.

3.4. Axioms of Existence and Maximality of local states

Given $D \in \mathcal{D}$, for each $t \in \text{TYP}$ let $LS_t = \{S_1, \ldots, S_n\}$ be the set of all the local states of type t. We assume the following *existence axiom:*

$$\mathbf{Ex}_t. \qquad AG(S_1 \vee \ldots \vee S_n).$$

For each $S \in LS_t$ and for each propositional symbol $a \in \text{wff}_t$ if $a \notin S$ we assume the following *maximality axiom:*

$$\mathbf{max}_t[S, a]. \qquad AG \neg (S \wedge a).$$

With $\mathbf{Max}_t$ we denote the set of all the maximality axioms of type t. ■

3.5. DEFINITION: For $D \in \mathcal{D}$, $t \in \text{TYP}$ and $N \in \{AX, EX, \neg AX, \neg EX\}$, each wff_t of the kind $S \supset NS'$ where $S, S' \in LS_t$, is called *unitary local formula* (of type t). With $\mathbf{ULF}_t$ we denote the set of unitary local formulas of type t. ■

3.6. *Example:* With reference to the system of examples 1.1 and 1.5, the following ones are unitary local formulas of type t_{p_1}:

$$b \wedge e \wedge g \supset EX(c \wedge d \wedge *_{p_3}),$$

$$a \wedge e \wedge *_{p_3} \supset AX(a \wedge d \wedge *_{p_3}), \qquad c \wedge d \wedge g \supset EX(b \wedge d \wedge *_{p_3}).$$

As we shall see, not all of these $\text{wff}_{t_{p_1}}$ are theorems (*i.e.* not all of these $wff_{t_{p_1}}$ correspond to an effective one step behaviour of the system). The formula $b \wedge e \wedge g \supset EX\, c$ is not a unitary local formula of type t_{p_1} as the formula c is not a unitary local state. ■

The idea of unitary local formulas is that of formalizing the one step behaviours of the subsystems of D resulting by the decomposition function Dec. To give a precise notion of such one step behaviours we equip the logic with a set of axioms called Unitary Local Axioms. Each of these axioms has the form $S \supset EXS'$ or $S \supset \neg EXS'$.

A formula $S \supset EXS'$ with $S \neq S'$ is a unitary local axiom if and only if the changes respect the behaviour graph of the interested parts and agree with the relations M and R. A formula $S \supset EXS$ is a unitary local axiom if and only if there is no $S' \neq S$ such that $S \supset EXS'$ is a unitary local axiom. Finally, a formula $S \supset \neg EXS'$ is a unitary local axiom if and only if $S \supset EXS'$ is not an axiom.

More precisely, we have the following definition.

3.7. DEFINITION: For $D \in \mathcal{D}$ and $t_p \in \mathrm{TYP}$ (the type associated to part p), a unitary local formula $u \in \mathbf{ULF}_{t_p}$ is a *unitary local axiom* (of type t_p) iff:

(*a*) $u = S \supset EXS'$ and one of the two following conditions is satisfied:

1. (i) $S \neq S'$,

(ii) for each $p' \in \mathrm{Dec}(p).P$, if $a_1, a_2 \in p'$, $a_1 \neq a_2$, $a_1 \in S$, $a_2 \in S'$, then $(a_1, a_2) \in b'$, where b' is the behavior graph of p',

(iii) if $a_1 \in p'_1$, $a_2 \in p'_2$, $p'_1 \neq p'_2$, $p'_1, p'_2 \in \mathrm{Dec}(p).P$ and $(a_1, a_2) \in \mathrm{Dec}(p).M$, then $a_1 \in S \Rightarrow a_2 \notin S'$,

(iv) if $(a_1, a_2) \in \mathrm{Dec}(p).R$, $a_1, a_2 \in S$, then $a_1 \notin S' \Leftrightarrow a_2 \notin S'$,

(v) if $(a_1, a_2) \in \mathrm{Dec}(p).R$, $a_1 \in S$, $a_2 \notin S$, then $a_1 \in S'$,

2. $S = S'$ and for any other $S'' \neq S$ the pair S, S'' does not verify 1.

(*b*) $u = S \supset \neg EXS'$ and conditions 1 and 2 for $u' = S \supset EXS'$ are not satisfied.

We call $\mathbf{ULA}_{t_p}$ the set of unitary local axioms of type t_p. ■

3.8. *Example:* Let us consider the system in figure 3.

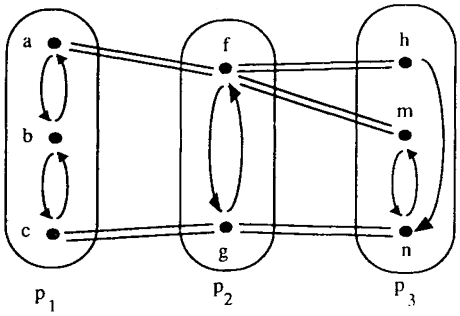


Figure 3

Let us consider the local states of type t_{p_2} $a \wedge f \wedge h$, $*_{p_1} \wedge g \wedge m$, $c \wedge g \wedge n$, $b \wedge f \wedge n$; the unitary local formulas of type t_{p_2} $a \wedge f \wedge h \supset EX\,(*_{p_1} \wedge g \wedge m)$,

$a \wedge f \wedge h \supset EX\, c \wedge g \wedge n$ are local axioms of type t_{p_2}, whereas

$$a \wedge f \wedge h \supset EX\, a \wedge f \wedge n$$

is not a $\mathbf{ULA}_{t_{p_2}}$ as condition 1-iv of definition 3.7 is not satisfied. ■

3.9. *Example:* The system in figure 4 shows a situation in which we have an axiom of the kind $S \supset EX\, S$, namely $a \wedge b \supset EX\, a \wedge b$. ■

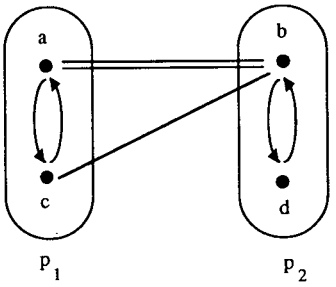


Figure 4

3.10. DEFINITION: We call Local Time Theory of a system D, or $\mathbf{LTT}_D$, the theory of **TTL** with the syntax given by 3.1 and, for each type $t \in \mathrm{TYP}$, $\mathbf{Ex}_t$, $\mathbf{Max}_t$ and $\mathbf{ULA}_t$ as mathematical axioms. We call *local theorems* the theorems of $\mathbf{LTT}_D$. ■

We have seen that, for a system D and each type t_p, the set wff_{t_p} corresponds to the set of temporal formulas relative to the subsystem $\mathrm{Dec}(p)$; this means that the well formed formulas of type t_p do not refer to a global concept of time but to a local one, *i.e.* to the time of the subsystem $\mathrm{Dec}(p)$. Therefore, we have a way to deal with local times, and this justifies the choice of the name $\mathbf{LTT}_D$ for the theory.

3.11. *Remark* (*On completeness of* $\mathbf{LTT}_D$) : Completeness of $\mathbf{LTT}_D$ (in the sense of completeness theorem) follows immediately from the completeness of *UB*; in fact, for each $t_p \in \mathrm{TYP}$ we have a theory of *UB* obtained by adding a finite set of axioms, namely maximality, existence and unitary local axioms, to *UB*. ■

Now we have to show that the proposed theories $\mathbf{LTT}_D$ are adequate for the formalization of distributed systems without any assumption of global time. The first step in showing such an adequacy consists in proving that, for a system D, $\mathbf{LTT}_D$ is a consistent theory. By classical results on temporal logics, it is sufficient to exhibit a model for $\mathbf{LTT}_D$.

3.12. DEFINITION (*Syntactic interpretation*): Let $D \in \mathcal{D}$ and let $\mathbf{LTT}_D$ be the corresponding theory with $\mathrm{TYP} = \{t_1, \ldots, t_n\}$. We call syntactic interpretation for $\mathbf{LTT}_D$ the structure $\mathcal{H}_D = \langle \mathcal{H}_{t_1}, \ldots, \mathcal{H}_{t_n} \rangle$ with for $t \in \mathrm{TYP}$, $\mathcal{H}_t = \langle WH_t, NH_t, PH_t \rangle$, where:

WH_t is LS_t, the set of local states of type t,

$(S, S') \in NH_t \Leftrightarrow (S \supset EX\,S') \in \mathbf{ULA}_t$,

$PH_t : WH_t \to 2^{\mathrm{PROP}}$ with $\alpha \in PH_t(S) \Leftrightarrow \alpha \in S$ for $S \in WH_t$. ■

The syntactic interpretation $\mathcal{H}_D$ is our candidate to be a model for $\mathbf{LTT}_D$.

3.13. THEOREM: *For each $D \in \mathcal{D}$ the syntactic interpretation $\mathcal{H}_D$ is a model for $\mathbf{LTT}_D$.*

Proof: It is sufficient to show that, for each type $t \in \mathrm{TYP}$ and for each mathematical axiom α of type t, $\mathcal{H}_D \underset{t}{\models} \alpha$. We have four cases:

1. $\alpha \in \mathbf{ULA}_t$ and $\alpha = S \supset EX\,S'$; then $\mathcal{H}_D \underset{t}{\models} \alpha$ by construction;

2. $\alpha \in \mathbf{ULA}_t$ and $\alpha = S \supset \neg\, EX\,S'$;

$$\mathbf{LTT}_D \underset{t}{\vdash} \alpha \Leftrightarrow \mathbf{LTT}_D \underset{t}{\nvdash} S \supset EX\,S' \Leftrightarrow (S, S') \notin NH_t$$

$$\Leftrightarrow (\forall S''\,(S, S'') \in NH_t \Rightarrow \mathcal{H}_D, S'' \underset{t}{\models} \neg\, S') \Leftrightarrow \mathcal{H}_D \underset{t}{\models} S \supset \neg\, EX\,S';$$

3. α is $\mathbf{Ex}_t$, *i.e.* $\alpha = AG(S_1 \vee \ldots \vee S_k)$; then

$$\mathcal{H}_D \underset{t}{\models} \alpha \Leftrightarrow \forall S \in S \in WH_t (\mathcal{H}_D, S \underset{t}{\models} S_1 \vee \ldots \vee S_k)$$

$$\Leftrightarrow \forall S \in WH_t\ (\mathcal{H}_D, S \underset{t}{\models} S_1 \text{ or} \ldots \text{or } \mathcal{H}_D, S \underset{t}{\models} S_k),$$

that holds by construction;

4. α is $\mathbf{max}_t[S, a]$, *i.e.* $\alpha = AG \neg\, (S \wedge a)$;

$\mathcal{H}_D \underset{t}{\models} AG \neg\, (S \wedge a) \Leftrightarrow \forall S' \in WH_t\, \mathcal{H}_D, S' \underset{t}{\models} \neg\, (S \wedge a)$; we have two cases:

(i) $S = S'$, then $\mathcal{H}_D, S' \underset{t}{\models} \neg\, a$ (as $a \notin S$) and therefore $\mathcal{H}_D, S' \underset{t}{\models} \neg\, (S \wedge a)$,

(ii) $S \neq S'$, then $\mathcal{H}_D, S' \underset{t}{\models} \neg\, S$ and therefore $\mathcal{H}_D, S' \underset{t}{\models} \neg\, (S \wedge a)$. ■

From this theorem we have immediately the following corollary.

3.14. COROLLARY: *For each $D \in \mathcal{D}$ the theory $\mathbf{LTT}_D$ is consistent.* ■

Now we can show that the syntactic interpretations is not merely a model but the most general model.

3.15. THEOREM: *For each* $D \in \mathcal{D}$, $\mathcal{H}_D$ *is the most general model, i.e. for* $t \in \mathrm{TYP}$, $\alpha \in \mathrm{wff}_t$ *and for each model* $\mathcal{M}$, $\mathcal{H}_D \models_t \alpha$ *implies* $\mathcal{M} \models_t \alpha$.

Proof: See appendix. ■

This theorem has some interesting consequences.

3.16 COROLLARY: For each $D \in \mathcal{D}$, $t \in \mathrm{TYP}$ and $\alpha \in \mathrm{wff}_t$, $\mathbf{LTT}_D \vdash_t \alpha$ iff $\mathcal{H}_D \models_t \alpha$.

Proof: From the completeness of $\mathbf{LTT}_D$ we have $\mathbf{LTT}_D \vdash_t \alpha$ iff $\models_t \alpha$, and therefore the thesis follows immediately from theorem 3.15. ■

This result states that the problem of theorem proving in $\mathbf{LTT}_D$ can be reduced to model checking on the model $\mathcal{H}_D$. Now it is already known that the formal system *UB* is decidable, but this result is of purely theoretical interest as the complexity of such a decision procedure belongs to $\mathcal{E}xp$-time. Now we can use a result of Danelutto and Masini [6], adapting it to the typed case.

3.17. PROPOSITION: *For each* $D \in \mathcal{D}$, $t \in \mathrm{TYP}$ *and* $\alpha \in \mathrm{wff}_t$, *the model checking procedure is in* $\mathcal{P}$*-time, more precisely the procedure to check* $\mathcal{H}_D \models_t \alpha$ *is bounded by* $O(\#\alpha \times (\#LS_t)^3)$. ■

By showing that theorem proving is reducible to model checking we have given an alternative decision procedure for $\mathbf{LTT}_D$, which, moreover, is in $\mathcal{P}$-time.

3.18. COROLLARY: *For each* $D \in \mathcal{D}$, *there is a polynomial-time bounded decision algorithm for* $\mathbf{LTT}_D$. ■

The last result for $\mathbf{LTT}_D$ is given by the following proposition.

3.19. PROPOSITION: *For each* $D \in \mathcal{D}$, $t \in \mathrm{TYP}$ *and* $\alpha \in \mathrm{wff}_t$ *at least one of the following assertions is true:*

1. $\mathbf{LTT}_D \vdash_t \alpha$,
2. $\mathbf{LTT}_D \vdash_t \neg \alpha$,
3. *there is a local state* $S \in LS_t$ *s.t.* $\mathbf{LTT}_D \vdash_t S \supset \alpha$.

Proof: The proof follows immediately from the equivalence of truth in the syntactic model $\mathcal{H}_D$ and provability in $\mathbf{LTT}_D$. In $\mathcal{H}_D$ one of the following

facts holds:

1. α is true w.r.t. t, *i.e.* $\mathscr{H}_D \underset{t}{\models} \alpha$, and therefore $\mathbf{LTT}_D \underset{t}{\vdash} \alpha$,

2. α is false w.r.t. t, *i.e.* $\mathscr{H}_D \underset{t}{\models} \neg\alpha$, and therefore $\mathbf{LTT}_D \underset{t}{\vdash} \neg\alpha$,

3. α is satisfiable w.r.t. t, *i.e.* there is a local state S s.t. $\mathscr{H}_D, S \underset{t}{\models} \alpha$, then there is a local state S s.t. $\mathscr{H}_D \models S \supset \alpha$, and therefore there is a local state S s.t. $\mathbf{LTT}_D \underset{t}{\vdash} S \supset \alpha$. ■

This proposition guarantees that our formalization is good, *i.e.* for each type t and for each assertion α formalizable within our system we can always decide whether with respect to t is valid or its negated is valid or there is a local state S such that $S \supset \alpha$ is valid.

3.20. *Example:* Let us consider the system D in figure 5.

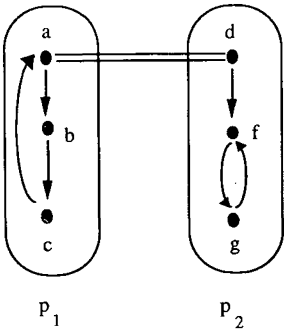


Figure 5

Using 3.7 to build the set of unitary local axioms of type t_{p_1} and t_{p_2} we obtain the syntactic model $\mathscr{H}_D = \langle \mathscr{H}_{t_{p_1}}, \mathscr{H}_{t_{p_2}} \rangle$ with $\mathscr{H}_{t_{p_1}}$, $\mathscr{H}_{t_{p_2}}$ as in figure 6.

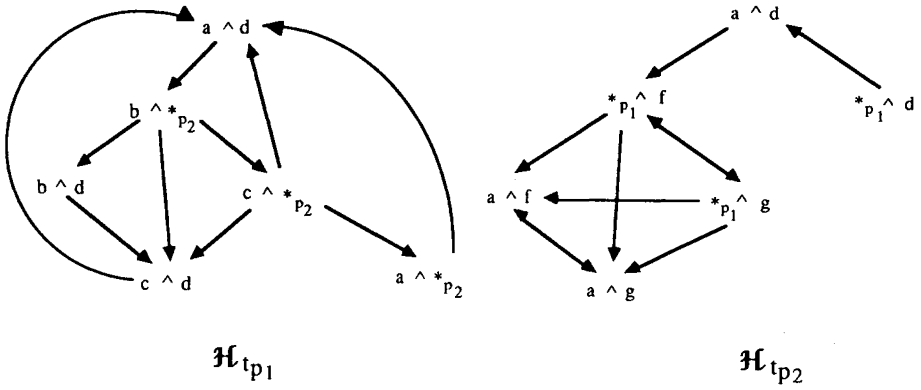
For example in $\mathscr{H}_{t_{p_1}}$ we have the arc $(a \wedge d, b \wedge *_{p_2}) \in NH_{t_{p_1}}$ because:

(i) $a \wedge d$ and $b \wedge *_{p_2}$ are local states of type t_{p_1},

(ii) (a, b) is an arc of $b_{p_1} \in \mathrm{Dec}_D(p_1).B$ and $(d, *_{p_2})$ is an arc of $b_{p_2} \in \mathrm{Dec}_D(p_1).B$,

(iii) $(a, d) \in \mathrm{Dec}_D(p_1).R$.

Now, by 3.7, we have that $\mathbf{LTT}_D \underset{t_{p_1}}{\vdash} a \wedge d \supset EX\, b \wedge *_{p_2}$, and therefore, by 3.12, that $(a \wedge d, b \wedge *_{p_2}) \in NH_{t_{p_1}}$.



$\mathcal{H}_{t_{p_1}}$ $\mathcal{H}_{t_{p_2}}$

Figure 6

Using corollary 3.16 we have:

(i) $\mathbf{LTT}_D \underset{t_{p_1}}{\vdash} a \wedge d \supset AX(\neg a \equiv \neg d)$,

(ii) $\mathbf{LTT}_D \underset{t_{p_1}}{\vdash} a \wedge \neg d \supset AX a$,

(iii) $\mathbf{LTT}_D \underset{t_{p_1}}{\vdash} \neg a \wedge d \supset AX d$,

(iv) $\mathbf{LTT}_D \underset{t_{p_1}}{\vdash} c \wedge d \supset EF(b \wedge *_{p_2})$.

From the previous facts we obtain $\mathcal{H}_D \underset{t_{p_1}}{\models} AG\,AF(a \wedge d)$ and therefore by corollary 3.16 $\mathbf{LTT}_D \underset{t_{p_1}}{\vdash} AG\,AF(a \wedge d)$. Now we can observe that

$$\mathcal{H}_D \underset{t_{p_2}}{\models} \neg AG\,AF(a \wedge d) \text{ (or equivalently } \mathcal{H}_D \underset{t_{p_2}}{\models} EF\,EG \neg (a \wedge d)),$$

i.e. $\mathbf{LTT}_D \underset{t_{p_2}}{\vdash} \neg AG\,AF(a \wedge d)$, that is we have exhibited a wff $\alpha = AG\,AF(a \wedge d)$ such that α is a local theorem w.r.t. type t_{p_1} and its negated $\neg \alpha$ is a local theorem w.r.t. type t_{p_2}. ■

3.21. *Example (About the meaning of relations R and M):* Let us consider a system D. The following ones are local theorems of $\mathbf{LTT}_D$:

1. for each pair $(a, a') \in R$ with $a \in p$ and $a' \in p'$,

(i) $\mathbf{LTT}_D \underset{t_{p'}}{\vdash} a \wedge a' \supset AX(\neg a \equiv \neg a')$,

(ii) $\mathbf{LTT}_D \underset{t_{p'}}{\vdash} a \wedge \neg a' \supset AX a$,

(iii) $\mathbf{LTT}_D \underset{t_{p'}}{\vdash} \neg a \wedge a' \supset AX a'$,

2. for each $(a, a') \in M$ with $a \in p$ and $a' \in p'$,

(i) $\mathbf{LTT}_D \underset{t_p}{\vdash} AG \neg (a \wedge a')$,

(ii) $\mathbf{LTT}_D \underset{t_p}{\vdash} \neg a \wedge a' \supset AX \neg a$.

The proof of 1 is given by inspection of the syntactic model $\mathscr{H}_{t_p}$. To prove 1 (i) let us consider a generic world S of $\mathscr{H}_{t_p}$ s.t. $a, a' \in S$ (*i.e.* $\mathscr{H}, S \underset{t_p}{\models} a \wedge a'$) and the set of all the worlds S' s.t. $(S, S') \in NH_{t_p}$ (*i.e.* $\mathbf{LTT}_D \underset{t_p}{\vdash} S \supset EXS'$). By 3.7, for such an S', we have that $a \notin S'$ iff $a' \notin S'$, *i.e.* $\mathscr{H}, S' \underset{t_p}{\models} \neg a \equiv \neg a'$. In such a way we have shown that for each word S,

$$\mathscr{H}, S \underset{t_p}{\models} a \wedge a' \supset AX(\neg a \equiv \neg a'), \text{ i.e. } \mathscr{H}_D \underset{t_p}{\models} a \wedge a' \supset AX(\neg a \equiv \neg a')$$

and, by corollary 3.16, $\mathbf{LTT}_D \underset{t_{p'}}{\vdash} a \wedge a' \supset AX \neg a \equiv \neg a'$, that is our thesis. The proofs of 1 (ii) and 1 (iii) are analogous. To prove 2 (i) it is sufficient to observe that there is no local state S of type t_p such that $a, a' \in S$, *i.e.* for each world S, $\mathscr{H}, S \underset{t_p}{\models} \neg (a \wedge a')$, and therefore $\mathscr{H}_{t_p} \underset{t_p}{\models} AG \neg (a \wedge a')$. The proof of 2 (ii) is analogous to the proof of 2 (i). ■

Note that our formalization does not depend on any assumption on real time, including an assumption of existence of clocks. Our idea is that the time flow of each subsystem D' is given by the execution of phase transitions in the parts of D'. If D' is in the current local configuration C, every parallel execution of a nonempty set of possible phase transitions of D' with respect to C gives a next time local configuration. In other words, the time flow for the subsystem D' is given by the changes of its local configurations. Such a point of view agrees with the rules given to obtain the set of local axioms of the kind $S \supset EXS'$ with $S \neq S'$. A problem arises from the fact that we admit the existence of axioms of the kind $S \supset EXS$, *i.e.* we admit that there may be no change in the current local state but the time runs. In order to clarify this point we state the following proposition.

3.22. PROPOSITION: *For each type t and for each local state S of type t*

$$\mathbf{LTT}_D \underset{t}{\vdash} S \supset EXS \quad \Rightarrow \quad \mathbf{LTT}_D \underset{t}{\vdash} S \supset AXS.$$

Proof: It follows immediately from definition of $\mathbf{ULA}_t$. If $\mathbf{LTT}_D \vdash_t S \supset EXS$, then for each other S' not $\mathbf{LTT}_D \vdash_t S \supset EXS'$; this implies that in $\mathscr{H}_t$ there is one and only one arc $(S, S) \in NH_t$, and then $\mathbf{LTT}_D \vdash_t S \supset AXS$. ■

Using the previous proposition we can easily show that

$$\mathbf{LTT}_D \vdash_t S \supset EXS \Leftrightarrow \mathbf{LTT}_D \vdash_t S \supset AGS.$$

Therefore, we may conclude that the time flow of a subsystem of a distributed system is given by the observable changes in its local configurations; moreover, if no changes are possible from a given local configuration C, then it is assumed that time runs whereas the subsystem is blocked in C.

4. THEORIES OF TTL FOR DISTRIBUTED SYSTEMS WITH LOCAL AND GLOBAL TIMES

Consider the system D in figure 7 and assume that a is the current phase of part p_1.

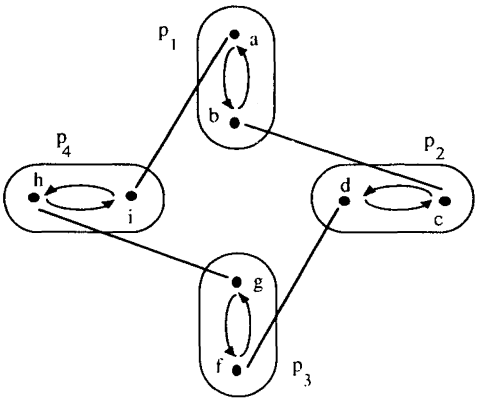


Figure 7

It is easy to see that there is only one global configuration containing phase a, namely $\{a, c, f, h\}$ that is a deadlock global configuration, *i.e.* the system may only remain forever in it. As a consequence we have that the following assertion is true: if part p_1 is in the current phase a then p_1 will remain in a forever (*i.e.* a is a deadlock phase for p_1). On the other hand,

we have $\mathbf{LTT}_D \underset{t_{p_1}}{\vdash} a \supset EF \neg a$, namely w.r.t. $\mathbf{LTT}_D$ a is not a deadlock phase for p_1. This is due to the fact that our formalization exploits only partial (local) knowledge of the system. Now one may ask whether it is possible to compose the local theorems of $\mathbf{LTT}_D$ in order to establish that, globally, phase a is a deadlock phase for part p_1.

The general question is: "given $D \in \mathscr{D}$, is it possible to extend $\mathbf{LTT}_D$ in order to formalize the local behavior as well as the global one, and moreover to obtain the global behavior by composition of the local ones?". This section is devoted to give a positive answer to the question. As a result, for a system D we shall have a new theory called $\mathbf{LGTT}_D$ (Local and Global Time Theory of D) which is a conservative extension of $\mathbf{LTT}_D$, namely which contains $\mathbf{LTT}_D$ plus a set of inference rules to compose local theorems in order to obtain global ones.

Before introducing $\mathbf{LGTT}_D$ we want to make clear our idea of the *time flow* for an entire system. As each subsystem is itself a distributed system, we simply extend our point of view of time flow for subsystems to the whole system, namely we assume that the (global) time flow of a system is given by the observable changes in its global configurations. If no changes are possible from a given global configuration C the (global) time runs indefinitely whereas the system is blocked in C.

In the rest of this section we assume that the considered system D is a quintuple $\langle A, P, B, M, R \rangle$.

4.1. Syntax of $\mathbf{LGTT}_D$

It is the syntax given in 2.1 for **TTL** with the following specific set of types:

$$\mathrm{TYP} = \{ t_p : p \in P \} \cup \{ G \},$$

where the types $t \neq G$ are called *local types* and G is a distinguished type called *global type*, the following set of propositional symbols:

$$\mathrm{Prop} = \bigcup_{p \in P} \mathrm{Dec}_D(p) . A$$

and observation function O_{LG}:

$$O_{LG}(a) = O_L(a) \cup \{G\} \qquad \text{for} \quad a \in A$$
$$O_{LG}(*_p) = O_L(*_p) \qquad \text{for} \quad *_p \in \text{PROP-}A,$$

where O_L is the observation function for $\mathbf{LTT}_D$. ■

All the features of $\mathbf{LTT}_D$ are carried on to $\mathbf{LGTT}_D$, *i.e.* $\mathbf{LGTT}_D$ restricted to the local types coincides with $\mathbf{LTT}_D$, namely, for each type $t \neq G$, $\mathbf{LTT}_D \vdash_t \alpha$ iff $\mathbf{LGTT}_D \vdash_t \alpha$. Moreover $\mathbf{LGTT}_D$ is endowed with new mathematical axioms and inference rules.

Following the approach of section 3, to type G we associate a set of wff of type G, called global states, that correspond to global configurations.

4.2. DEFINITION (*Global States*): Given $D \in \mathcal{D}$, let $\{a_{i_1}, \ldots, a_{i_n}\}$ be a global configuration. The wff_G $a_{i_1} \wedge \ldots \wedge a_{i_n}$ is called a *global state*. We call GS the set of all global states in $\mathbf{LGTT}_D$. ■

Related to the concept of global state is the notion of *projection*.

4.3. DEFINITION: Given $D \in \mathcal{D}$, let $\Sigma = a_1 \wedge \ldots \wedge a_n$ be a global state and let t be a local type; with $\pi_t[\Sigma]$ (*projection* of Σ w.r.t. type t) we denote the local state S of type t where for each $a_j \in \Sigma$ if $t \in O_{LG}(a_j)$ then $a_j \in S$. ■

As done for the local case, we add a set of axioms to formalize the properties enjoyed by global states.

4.4. Axioms of existence and maximality of global states

For $D \in \mathcal{D}$ let $GS = \{\Sigma_1, \ldots, \Sigma_n\}$ be the set of all global states.

We have the following *existence axioms*:

$$\mathbf{Ex}_G. \qquad AG(\Sigma_1 \vee \ldots \vee \Sigma_n).$$

For each $\Sigma \in GS$ and for each propositional symbol $a \in \text{wff}_G$, if $a \notin \Sigma$ we assume the following *maximality axiom*:

$$\mathbf{max}_G[\Sigma, a]. \qquad AG\neg(\Sigma \wedge a).$$

With $\mathbf{Max}_G$ we denote the set of all the maximality axioms of type G. ■

In section 3, for each distributed system D we have introduced a set of formulas called Unitary Local Formulas; a particular subset of them has been taken as proper axioms of the theory $\mathbf{LTT}_D$. We have shown that these local axioms are a sufficient base to formalize distributed systems from a

local point of view. The question is whether there is a global correspondent of unitary local axioms, *i.e.* a set of global formulas that may be chosen as an adequate base for the global formalization of distributed systems. In [6] Danelutto and Masini show how to build such a set of global formulas but in a framework without any assumption of local times. Now the question is whether such formulas may be obtained by composition of local formulas. In a logical formal system a basic mechanism to compose formulas to obtain other formulas is that of inference rules. In our specific case we have to introduce some *multityped inference rules* (*i.e.* inference rules over formulas of differents types) of the kind:

$$\frac{\mathbf{LGTT}_D \underset{t_1}{\vdash} \beta_1 \ldots \mathbf{LGTT}_D \underset{t_r}{\vdash} \beta_r}{\mathbf{LGTT}_D \underset{G}{\vdash} \alpha}$$

where the $\beta_1, \ldots, \beta_n$ are local formulas. The intended meaning of such an inference rule is that the global formula α is obtained by composition of the local formulas $\beta_1, \ldots, \beta_n$. We will show that, for our aims, it is sufficient to restrict the multityped inference rules to unitary formulas.

4.5. DEFINITION: Let $N \in \{AX, EX, \neg AX, \neg EX\}$; given $D \in \mathcal{D}$, each wff_G of the kind $\Sigma \supset N\Sigma'$,with $\Sigma, \Sigma' \in GS$, is called *unitary global formula*. We call **UGF** the set of unitary global formulas. ■

4.6. DEFINITION: The function $\Delta : GS \times GS \to 2^{\text{TYP}}$ defined as

$$\Delta(\Sigma, \Sigma') = \{ t_p : t_p \in \text{TYP} - \{G\}, \exists a', a'' \text{ s.t. } a', a'' \in p, a' \in \Sigma, a'' \in \Sigma', a' \neq a'' \text{ and } t_p \in O_{LG}(a') \cup O_{LG}(a'') \}$$

is called *type difference function* of Σ and Σ'. ■

Let us discuss the meaning of the type difference function; let us take two global states $\Sigma = Z \wedge Y$, $\Sigma' = Z' \wedge Y$, where $a \in Z$ and $a' \in Z'$ implies that $a \neq a'$; the extremal cases are given by $Z = Z' = \varnothing$, (*i.e.* $\Sigma = \Sigma'$), and $Y = \varnothing$, (*i.e.* all the atomic formulas in Σ are different from the atomic formulas in Σ'). Note that Z and Z' must have the same number of atomic formulas. Let us consider an atomic formula $a \in Z$, by definition of global state in Z' there is another atomic formula a' s. t. a, a' belong to the same part p. In such a case we assert that the type t_p belong to $\Delta(\Sigma, \Sigma')$ as part p is interested into the difference between Z and Z'. Now let us consider an atomic formula $b \in Y$, s. t. b belongs to part q; in such a case we have that part q is not directly interested into the difference between Σ and Σ' (b belongs to both Σ and Σ').

We would expect that type t_q does not belong to $\Delta(\Sigma, \Sigma')$, but, also in this case, we admit that type t_q belongs to $\Delta(\Sigma, \Sigma')$ if there is at least an atomic formula c in Z or Z' s.t. $t_q \in O_{LG}(c)$, *i.e.* in the case that part q is *indirectly* interested into the difference between Z and Z'. Note that if $\Sigma = \Sigma'$, *i.e.* $Z = Z' = \varnothing$, we have that $\Delta(\Sigma, \Sigma') = \varnothing$ as there is no difference between Σ and Σ'.

The following example shows the construction of Δ in a concrete case.

4.7. *Example:* Let us suppose we have the system in figure 8.

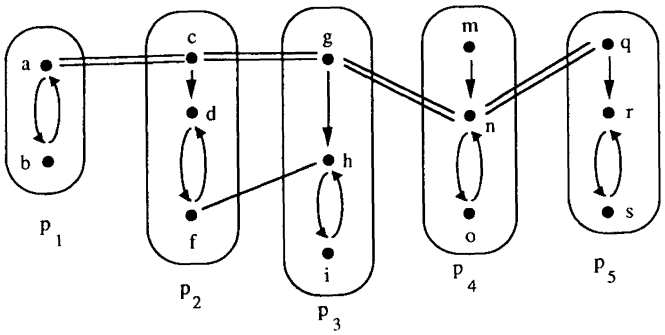


Figure 8

Let $\Sigma = a \wedge c \wedge g \wedge m \wedge q$ and $\Sigma' = b \wedge d \wedge h \wedge m \wedge q$ be two global states; by applying the previous definition we have $\Delta(\Sigma, \Sigma') = \{t_{p_1}, t_{p_2}, t_{p_3}, t_{p_4}\}$; Σ and Σ' have a subformula in common, *i.e.* $Y = m \wedge q$, and two subformulas which are different, *i.e.* $Z = a \wedge c \wedge g$ in Σ and $\Sigma' = b \wedge d \wedge h$ in Σ'. With respect to the subformulas Z and Z' we have:

(i) $a, b \in p_1 \Rightarrow t_{p_1} \in \Delta(\Sigma, \Sigma')$,

(ii) $c, d \in p_2 \Rightarrow t_{p_2} \in \Delta(\Sigma, \Sigma')$,

(iii) $g, h \in p_3 \Rightarrow t_{p_3} \in \Delta(\Sigma, \Sigma')$.

By definition we have also that type t_{p_4} belongs to $\Delta(\Sigma, \Sigma')$ even though part p_4 remains in the same phase m w.r.t. the global states Σ and Σ'. This happens because $t_{p_4} \in O_{LG}(g) \cup O_{LG}(h)$, *i.e.* part p_4 is indirectly interested in the difference between Z and Z'. On the other hand type t_{p_5} does not belong to $\Delta(\Sigma, \Sigma')$ as part p_5 cannot observe any phase in the subformulas Z and Z'. ■

We give now the inference rules to compose local behaviours.

4.8. Inference rules

Given $D \in \mathscr{D}$, let Σ and Σ' be two global states with $\Sigma \neq \Sigma'$; the following are inference rules of the theory $\mathbf{LGTT}_D$:

Rule XG1:

$$\frac{\forall t_p \ \forall a \ (t_p \in \mathrm{TYP},\ a \in \Sigma,\ a \in p \Rightarrow \mathbf{LGTT}_D \underset{t_p}{\vdash} \pi_{t_p}[\Sigma] \supset AX a)}{\mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset EX \Sigma.}$$

Rule XG2:

$$\frac{\forall t_p \ (t_p \in \Delta(\Sigma, \Sigma') \ \Rightarrow \ \mathbf{LGTT}_D \underset{t_p}{\vdash} \pi_{t_p}[\Sigma] \supset EX \pi_{t_p}[\Sigma'])}{\mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset EX \Sigma'}$$

Rule NXG1:

$$\frac{\exists t_p \exists a (t_p \in TYP,\ a \in \Sigma,\ a \in p,\ \mathbf{LGTT}_D \underset{t_p}{\vdash} \pi_{t_p}[\Sigma] \supset \neg AX a)}{\mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset \neg EX \Sigma}$$

Rule NXG2:

$$\frac{\exists t_p \ (t_p \in \Delta(\Sigma, \Sigma') \mathbf{LGTT}_D \underset{t_p}{\vdash} \pi_{t_p}[\Sigma] \supset \neg EX \pi_{t_p}[\Sigma'])}{\mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset \neg EX \Sigma'}$$ ■

4.9. DEFINITION: We call Local and Global Time Theory of a system D, or $\mathbf{LGTT}_D$, the theory of **TTL** with the syntax given by 4.1, which is a conservative extension of $\mathbf{LGTT}_D$ (namely such that for each type $t \neq G$ $\mathbf{LTT}_D \underset{t}{\vdash} \alpha$ iff $\mathbf{LGTT}_D \underset{t}{\vdash} \alpha$), with the axions $\mathbf{Ex}_G$ and $\mathbf{Max}_G$ and the inference rules *XG*1, *XG*2, *NXG*1, *NXG*2. We call *global theorems* the theorems of $\mathbf{LGTT}_D$ that hold w.r.t. type G. ■

Before showing that rules *XG*1, *XG*2, *NXG*1 and *NXG*2 are all what we need to infer global properties, we want to give some intuition on them. We shall consider only *XG*1 an *XG*2 as rules *NXG*1 and *NXG*2 assert simply that a wff_G $\Sigma \supset \neg EX \Sigma'$ is a global theorem iff we cannot infer $\Sigma \supset EX \Sigma'$ by applying rules *XG*1 and *XG*2. By rule *XG*1 we infer global theorems of the kind $\mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset EX \Sigma$. As we want to stick to our idea of time flow,

we expect that $\mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset EX\,\Sigma \Rightarrow \mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset AX\,\Sigma$, namely we expect that $\mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset EX\,\Sigma$ iff, for each part p, if a is the current phase of p w.r.t. Σ then p must remain forever in a.

4.10. *Example:* Let us consider the system in figure 9.

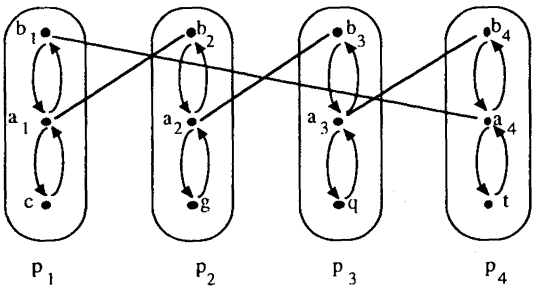


Figure 9

Let $\Sigma = b_1 \wedge b_2 \wedge b_3 \wedge b_4$ be a global state; in order to prove

$$\mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset EX\,\Sigma,$$

we have to show that for each type $t_{p_i}(1 \leqq i \leqq 4)$ we have

$$\mathbf{LGTT}_D \underset{t_{p_i}}{\vdash} \pi_{t_{p_i}}[\Sigma] \supset AX\,a$$

with $a \in \Sigma$, *i.e.* that $\mathbf{LGTT}_D \underset{t_{p_i}}{\vdash} *_{p_{i-1}} \wedge b_i \wedge b_{i+1} \supset AX\,b_i$ (sum and substraction are made modulo 4). The proof of these theorems is easily done by inspection on the syntactic model $\mathscr{H}_D$. ■

Rule *XG2* allows us to prove global theorems of the kind $\mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset EX\,\Sigma'$, with $\Sigma \neq \Sigma'$. The idea is that to prove such global theorems we have to check for local theorems w.r.t. the set of types in $\Delta(\Sigma, \Sigma')$. Such an approach is coherent with our idea that time flow is modelled by the observable changes in global configurations. The problem is to understand why we can limit ourselves to checking local theorems with types in the set $\Delta(\Sigma, \Sigma')$. Let us take as an example the system in figure 10.

Let us suppose that we want to prove that $\Sigma \supset EX\,\Sigma'$ is a global theorem with $\Sigma = a \wedge c \wedge f \wedge h$ and $\Sigma' = b \wedge d \wedge f \wedge h$. In this case

$$\Delta(\Sigma, \Sigma') = \{ t_{p_1}, t_{p_2}, t_{p_3} \}.$$

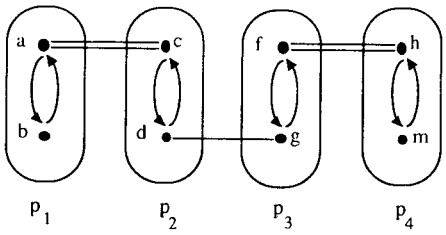


Figure 10

The following unitary formulas are unitary local axioms:

1. $a \wedge c \supset EX(b \wedge *_{p_2})$ w.r.t. type t_{p_1},
2. $a \wedge c \wedge *_{p_3} \supset EX(*_{p_1} \wedge d \wedge *_{p_3})$ w.r.t type t_{p_2},
3. $*_{p_2} \wedge f \wedge h \supset EX(d \wedge f \wedge h)$ w.r.t. type t_{p_3}.

By rule $XG2$ we obtain $\mathbf{LGTT}_D \vdash_G a \wedge c \wedge f \wedge h \supset EX(b \wedge d \wedge f \wedge h)$. Note that type $t_{p_4} \notin \Delta(\Sigma, \Sigma')$ and therefore we do not have to prove anything about local formulas of type t_{p_4}. ■

From the above example we see that rule $XG2$ cannot be extended to include parts which are not in $\Delta(\Sigma, \Sigma')$. Actually, $\pi_{t_{p_4}}[\Sigma] \supset EX\,\pi_{t_{p_4}}[\Sigma']$ where $\pi_{t_{p_4}}[\Sigma] = f \wedge h$ and $\pi_{t_{p_4}}[\Sigma'] = f \wedge h$, is not a local theorem (it holds $\mathbf{LGTT}_D \vdash_{t_{p_4}} f \wedge h \supset AX \neg h$). This agrees with the fact that considering local theorems w.r.t. type t_{p_4} would lead to force a dependency between parts p_4 and p_2 which does not exist.

With giving the inference rules we have completed the definition of the formal system $\mathbf{LGTT}_D$. Let us now prove consistency and completeness of such rules. The first theorem we prove is about consistency.

We can now prove that rules $XG1$, $XG2$, $NXG1$ and $NXG2$ offer a complete base to decide about provability of each global formula (obviously expressible in UB). We proceed in a way strongly similar to the one followed for the theories $\mathbf{LTT}_D$. First of all we show that it is possible to associate to each theory $\mathbf{LGTT}_D$ a finite Kripke model. Such a model will be a pair $\mathscr{H}_D^+ = \langle \mathscr{H}_D, \mathscr{H}_G \rangle$, with $\mathscr{H}_D$ the syntactic model seen for $\mathbf{LTT}_D$ and $\mathscr{H}_G$ a Kripke model for the global part of $\mathbf{LGTT}_D$. We shall see that the model $\mathscr{H}_G$ is built by using only formulas derivable by means of the inference rules $XG1$, $XG2$, $NXG1$ and $NXG2$. Successively, we shall show that each global formula α is provable in $\mathbf{LGTT}_D$ iff α is true in $\mathscr{H}_D^+$; in this way we shall obtain the completeness of rules $XG1$, $XG2$, $NXG1$, $NXG2$ in order to decide provability of global formulas.

4.11. *Remark* (*On completeness of* $\mathbf{LGTT}_D$): For local formulas see remark 3.11 on completeness of $\mathbf{LTT}_D$. For global formulas the question seems to be more complicated as such formulas are obtained by means of new inference rules (*XG*1, *XG*2, *NXG*1 and *NXG*2) which are not present in *UB*. But this is not a real difficulty. Actually, let us call $\mathscr{X}$ the set of unitary global formulas obtained by application of rules *XG*1, *XG*2, *NXG*1 and *NXG*2 and consider the theory $\mathbf{LGTT}^*(D)$ that is identical to $\mathbf{LGTT}_D$ for the local types and that has not the rules *XG*1, *XG*2, *NXG*1 and *NXG*2 but has directly the set $\mathscr{X}$ as axioms for the global part. In this theory all and only all the theorems of $\mathbf{LGTT}_D$ can be proved; moreover $\mathbf{LGTT}^*(D)$ is complete and this is sufficient to establish the completeness of $\mathbf{LGTT}_D$. ■

Now we extend the concept of syntactic interpretation given for $\mathbf{LTT}_D$ in order to consider also global formulas.

4.12. DEFINITION (*Syntactic interpretation*): Let $D \in \mathscr{D}$ and let $\mathbf{LGTT}_D$ be the corresponding theory with $\mathrm{TYP} = \{ t_1, \ldots, t_n, G \}$. We call syntactic interpretation for $\mathbf{LGTT}_D$ the structure $\mathscr{H}_D^+ = \langle \mathscr{H}_D, \mathscr{H}_G \rangle$, where $\mathscr{H}_D$ is the syntactic model of $\mathbf{LTT}_D$ and

$$\mathscr{H}_G = \langle WH_G, NH_G, PH_G \rangle,$$

where:

WH_G is GS, the set of global states,

$$(\Sigma, \Sigma') \in NH_G \quad \Leftrightarrow \quad (\mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset EX\, \Sigma'),$$

$PH_G : WH_G \to 2^{\mathrm{PROP}}$ with $\alpha \in PH_G(\Sigma) \Leftrightarrow \alpha \in \Sigma$, for $\Sigma \in WH_G$. ■

About $\mathscr{H}_D^+$ we have the following result.

4.13. THEOREM: *For each* $D \in \mathscr{D}$ *the syntactic interpretation* $\mathscr{H}_D^+$ *is a model for* $\mathbf{LGTT}_D$.

Proof: The proof for the local fragment of $\mathbf{LGTT}_D$ is the same given for theorem 3.13. Let us now examine the global fragment. The proof related to the axioms $\mathbf{Ex}_G$ and $\mathbf{Max}_G$ is analogous to the one given in 3.13 for the corresponding local axioms; we have only to examine the inference rule *XG*1, *XG*2, *NXG*1 and *NXG*2 and prove that these rules preserve truth in the syntactic interpretation $\mathscr{H}_D^+$.

Rule XG1: We have to prove that

$$(\forall t_p \forall a (t_p \in \mathrm{TYP},\ a \in \Sigma,\ a \in p \Rightarrow \mathscr{H}_D^+ \underset{t_p}{\models} \pi_{t_p}[\Sigma] \supset AX\, a)) \quad \Rightarrow \quad \mathscr{H}_D^+ \underset{t_p}{\models} \Sigma \supset EX\, \Sigma.$$

It holds that

$$(\forall t_p \forall a (t_p \in \mathrm{TYP},\ a \in \Sigma,\ a \in p \Rightarrow \mathscr{H}_D^+ \underset{t_p}{\models} \pi_{t_p}[\Sigma] \supset AX a))$$

$$\Rightarrow\ (\forall t_p \forall a (t_p \in \mathrm{TYP},\ a \in \Sigma,\ a \in p)$$

$$(\mathbf{LGTT}_D \underset{t_p}{\vdash} \pi_{t_p}[\Sigma] \supset AX a))\quad (\text{by definition of } \mathscr{H}_D^+)$$

$$\Rightarrow\ \mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset EX\,\Sigma\ \Rightarrow\ \mathscr{H}_D^+ \underset{t_p}{\models} \Sigma \supset EX\,\Sigma\ (\text{by rule } XG1).$$

Rule XG2: We have to prove that

$$(\forall t_p (t_p \in \Delta(\Sigma, \Sigma')\ \Rightarrow\ (\mathscr{H}_D^+ \underset{t_p}{\models} \pi_{t_p}[\Sigma] \supset EX \pi_{t_p}[\Sigma']))$$

$$\Rightarrow\ \mathscr{H}_D^+ \underset{t_p}{\models} \Sigma \supset EX\,\Sigma',\quad \text{with } \Sigma \neq \Sigma'.$$

It holds that

$$(\forall t_p \in \Delta(\Sigma, \Sigma')(\mathscr{H}_D^+ \underset{t_p}{\models} \pi_{t_p}[\Sigma] \supset EX \pi_{t_p}[\Sigma']))$$

$$\Rightarrow\ (\forall t_p \in \Delta(\Sigma, \Sigma')(\mathbf{LGTT}_D \underset{t_p}{\vdash} \pi_{t_p}[\Sigma] \supset EX \pi_{t_p}[\Sigma']))$$

$$\Rightarrow\ \mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset EX\,\Sigma'\ \Rightarrow\ \mathscr{H}_D^+ \underset{t_p}{\models} \Sigma \supset EX\,\Sigma'.$$

Rule NXG1: We have to prove that

$$(\exists t_p \exists a (t_p \in \mathrm{TYP},\ a \in \Sigma,\ a \in p,\ \mathscr{H}_D^+ \underset{t_p}{\models} \pi_{t_p}[\Sigma] \supset \neg\, EX a)$$

$$\Rightarrow\ \mathscr{H}_D^+ \underset{G}{\models} \Sigma \supset \neg\, EX\,\Sigma.$$

It holds that

$$(\exists t_p \exists a (t_p \in \mathrm{TYP},\ a \in \Sigma \text{ and } a \in p,\ \mathscr{H}_D^+ \underset{t_p}{\models} \pi_{t_p}[\Sigma] \supset \neg\, AX a)$$

$$\Rightarrow\ (\exists t_p \exists a (t_p \in \mathrm{TYP},\ a \in \Sigma,\ a \in p,\ \mathbf{LGTT}_D \underset{t_p}{\vdash} \pi_{t_p}[\Sigma] \supset \neg\, AX a))$$

$$\Rightarrow\ \mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset \neg\, EX\,\Sigma\ \Rightarrow\ \mathscr{H}_D^+ \underset{G}{\models} \Sigma \supset \neg\, EX\,\Sigma.$$

Rule NXG2: We have to prove that

$$(\exists t_p (t_p \in \Delta(\Sigma, \Sigma'), \mathscr{H}_D^+ \underset{t_p}{\models} \pi_{t_p}[\Sigma] \supset \neg EX \pi_{t_p}[\Sigma']) \Rightarrow \mathscr{H}_D^+ \underset{G}{\models} \Sigma \supset \neg EX \Sigma', \quad \text{with } \Sigma \neq \Sigma'.$$

It holds that

$$(\exists t_p (t_p \in \Delta(\Sigma, \Sigma'), \mathscr{H}_D^+ \underset{t_p}{\models} \pi_{t_p}[\Sigma] \supset \neg EX \pi_{t_p}[\Sigma'])) \Rightarrow (\exists t_p \in \Delta(\Sigma, \Sigma') (\mathbf{LGTT}_D \underset{t_p}{\vdash} \pi_{t_p}[\Sigma] \supset \neg EX \pi_{t_p}[\Sigma'])) \Rightarrow \mathbf{LGTT}_D \underset{G}{\vdash} \Sigma \supset \neg EX \Sigma' \Rightarrow \mathscr{H}_D^+ \underset{G}{\models} \Sigma \supset \neg EX \Sigma'. \blacksquare$$

Consistency of $\mathbf{LGTT}_D$ follows immediately.

4.14. COROLLARY: *For each $D \in \mathscr{D}$ the theory $\mathbf{LGTT}_D$ is consistent.* ■

We can also show that $\mathscr{H}_D^+$ is the most general model of $\mathbf{LGTT}_D$.

4.15. THEOREM: *For each $D \in \mathscr{D}$, $\mathscr{H}_D^+$ is the most general model,* i.e. *for $t \in \mathrm{TYP} \cup \{G\}$, $\alpha \in wff_t$ and for each model $\mathscr{M}$, $\mathscr{H}_D^+ \underset{t}{\models} \alpha$ implies $\mathscr{M} \underset{t}{\models} \alpha$.*

Proof: See in the appendix. ■

Now we obtain all the results seen for the theory $\mathbf{LTT}_D$ also for $\mathbf{LGTT}_D$. We may give such results only for the global formulas as for the local ones the results of section 3 remain obviously valid.

4.16. COROLLARY: *For each $D \in \mathscr{D}$, for each $\alpha \in wff_G$ $\mathbf{LGTT}_D \underset{G}{\vdash} \alpha$ iff $\mathscr{H}_D^+ \underset{G}{\models} \alpha$.* ■

4.17. PROPOSITION: *For each $wff_G \alpha$ the model checking procedure is in $\mathscr{P}$-time, more precisely the procedure to check whether $\mathscr{H}_D^+ \underset{G}{\models} \alpha$ is bounded by $O(\#\alpha \times (\#GS)^3)$.* ■

4.18. COROLLARY: *There is a $\mathscr{P}$-time bounded decision algorithm for $\mathbf{LGTT}_D$.* ■

The last result for $\mathbf{LGTT}_D$ is given by the following proposition (whose proof is similar to that of proposition 3.19).

4.19. PROPOSITION: *For each* $\alpha \in wff_G$ *at least one of the following assertions is true*:

1. $\mathbf{LGTT}_D \vdash_G \alpha$,
2. $\mathbf{LGTT}_D \vdash_G \neg \alpha$,
3. there is global state $\Sigma \in GS$ s. t. $\mathbf{LGTT}_D \vdash_G \Sigma \supset \alpha$. ■

By the proposition we have proved that our compositional approach is good.

5. CONCLUSIONS

We have shown that temporal logics are adequate to describe distributed systems on condition that a suitable typization of formulas is introduced. Actually, a distributed system can be formalized by means of typed formulas describing local properties. Global properties of the system can be obtained by using inference rules which relate local and global formulas. For the theories $\mathbf{LTT}_D$ and $\mathbf{LGTT}_D$ that we have introduced, we have proved the equivalence of theorem proving and model checking in the finite models $\mathscr{H}_D$ and $\mathscr{H}_D^+$, respectively. Therefore the theories $\mathbf{LTT}_D$ and $\mathbf{LGTT}_D$ are decidable in $\mathscr{P}$-time by model checking in $\mathscr{H}_D$ and $\mathscr{H}_D^+$.

On the case of the work that has been done a specification and verification methodology could be developed. Stepwise definition of distributed systems and system reconfiguration (*i. e.* adding and deleting parts) could actually be done by changing only local axioms and redemonstrating local properties of parts involved in the change.

REFERENCES

1. J. VAN BENTHEM, Modal Logic and Classical Logic, Bibliopolis, Napoli, 1985.
2. M. BEN-ARI, A. PNUELI and Z. MANNA, The Temporal Logic of Branching Time, *Acta Inform.*, 1983, *20*, pp. 207-226.
3. E. M. CLARKE, E. A. EMERSON and A. P. SISTLA, Automatic Verification of Finite-State Concurrent Systems Using Temporal Logic Specifications, *A.C.M. Trans. Prog. Lang. Syst.*, 1986, *8*, pp. 244-263.
4. E. M. CLARKE, O. GRUMBERG and R. P. KURSHAN, A Synthesis of Two Approaches for Verifying Finite State Concurrent Systems, "Logic at Botik '89", *Lect. Notes in Comput. Sci.*, 1989, *363*, Springer, Berlin, pp. 81-90.

5. E. M. CLARKE, D. E. LONG and K. L. MCMILLAN, Compositional Model Checking, "Fourth Annual Symposium on Logic in Computer Science", I.E.E.E. Computer Society Press, Washington, D.C., 1989, pp. 353-362.

6. M. DANELUTTO and A. MASINI, A Temporal Logic Approach to Specify and to Prove Properties of Finite State Concurrent Systems, "CSL'88", *Lecture Notes in Comput. Sci*, 1989, *385*, Springer, Berlin, pp. 63-79.

7. P. DEGANO, R. DE NICOLA and U. MONTANARI, A Distributed Operational Semantics for CCS Based on Condition/Event Systems, *Acta Inform.*, 1987, *26*, pp. 59-91.

8. E. A. EMERSON, Alternative Semantics for Temporal Logics, *Theoret. Comput. Sci.*, 1983, *26*, pp. 121-130.

9. E. A. EMERSON and E. M. CLARKE, Using Branching Time Temporal Logic to Synthesize Synchronization Skeletons, *Sci. Comput. Programming*, 1982, *2*, pp. 241-266.

10. E. A. EMERSON and J. Y. HALPERN, Decision Procedures and Expressiveness in the Temporal Logic of Branching Time, *J. Comput. System Sci.*, 1985, *30*, pp. 1-24.

11. E. A. EMERSON and J. Y. HALPERN, "Sometimes" and "Not Never" Revisited: On Branching Versus Linear Time Temporal Logic, *J. A.C.M.*, 1986, *33*, pp. 151-178.

12. E. A. EMERSON and C. L. LEI, Modalities for Model Checking: Branching Time Strikes Back, *12th A.C.M. Symposium on Principles of Programming Languages*, 1985, pp. 84-96.

13. E. A. EMERSON and A. P. SISTLA, Deciding Full Branching Time Logic, *Inform. and Control*, 1984, *61*, pp. 175-201.

14. P. ENJALBERT and M. MICHEL, Many-Sorted Temporal Logic for Multi-Process Systems, "Mathematical Foundations of Computer Science, 1984", *Lecture Notes in Comput. Sci., 176, Springer*, Berlin, 1984, pp. 273-281.

15. F. KRÖGER, Temporal Logic of Programs, *Springer*, Berlin, 1987.

16. L. LAMPORT, "Sometimes" is Sometimes "Not Never": On the Temporal Logic of Programs, *7th A.C.M. Symposium on Principles of Programming Languages*, 1980, pp. 174-185.

17. K. LODAYA and P. S. THIAGARAJAN, A Modal Logic for a Subclass of Event Structures, Automata Languages and Programming '87, *Lecture Notes in Comput. Sci.*, 1987, *267*, *Springer*, Berlin, pp. 290-303.

18. Z. MANNA and P. WOLPER, Synthesis of Communicating Process from Temporal Logic Specifications, *A.C.M. Trans. Prog. Lang. Syst.*, 1984, *6*, pp. 68-93.

19. A. MASINI, I Sistemi di Interazione: una proposta di formalizzazione logico-temporale e di realizzazione semanticamente corretta, *Tesi di Laurea in Scienze dell'Informazione*, Università di Pisa, 1986.

20. V. NGUYEN, A. DEMERS, D. GRIES and S. OWICKI, A Model and Temporal Proof System for Networks of Processes, *Distributed Computing*, 1986, *1*, pp. 7-25.

21. H. F. WEDDE, An Iterative and Starvation-Free Solution for a General Class of Distributed Control Problems Based on Interaction Primitives, *Theoret. Comput. Sci.*, 1983, *24*, pp. 1-20.

APPENDIX

MODEL PROPERTIES

We assume to have a system $D = \langle A, P, B, M, R \rangle \in \mathcal{D}$ and, correspondingly, to have the theory $\mathbf{LGTT}_D$ with $\mathrm{TYP} = \{t_1, \ldots, t_n, G\}$ as set of types. For the sake of simplicity we shall call *states of type t* both local states (where $t \neq G$) and global states (where $t = G$). A state will be denoted by the greek letter Ω, possibly indexed.

A1. LEMMA: *For each pair of states* Ω, Ω' *of type* t, *if* $\Omega \neq \Omega'$ *then* $\mathbf{LGTT}_D \vdash_t AG\neg(\Omega \wedge \Omega')$.

Proof: Let us take $\Omega' = a_1 \wedge \ldots \wedge a_n$ with $\Omega \neq \Omega'$; without loss of generality, we can assume that $a_1 \notin \Omega$, and then, by axiom $\mathbf{max}_t[\Omega, a_1]$ and using *UB* axioms and inference rules, we have:

$$\mathbf{LTT}_D \vdash_t AG\neg(\Omega \wedge a_1) \Rightarrow \mathbf{LTT}_D \vdash_t \neg(\Omega \wedge a_1)$$

$$\Rightarrow \mathbf{LTT}_D \vdash_t \neg(\Omega \wedge a_1) \vee \ldots \vee \neg(\Omega \wedge a_n)$$

$$\Rightarrow \mathbf{LTT}_D \vdash_t \neg(\Omega \wedge a_1 \wedge \ldots \wedge a_n) \Rightarrow \mathbf{LTT}_D \vdash_t AG\neg(\Omega \wedge \Omega'). \quad \blacksquare$$

A2. LEMMA: *Let* $\mathcal{M} = \langle \mathcal{M}_{t_1}, \ldots, \mathcal{M}_{t_n}, \mathcal{M}_G \rangle$ *be a model of* $\mathbf{LGTT}_D$ *and let* $t \in \mathrm{TYP}$; *then for each world w in* $\mathcal{M}_t$ *there is one and only one state* Ω *of type t s. t.* $\mathcal{M}, w \models_t \Omega$. *We will denote such unique state with* Ω_w.

Proof: Let w be a world of $\mathcal{M}_t$; by the axiom $\mathbf{Ex}_t AG(\Omega_1 \vee \ldots \vee \Omega_m)$ we have that $\mathcal{M}, w \models_t (\Omega_1 \vee \ldots \vee \Omega_m)$ and therefore at least one of the $\Omega_1 \ldots \Omega_m$, say Ω_j, must hold in w. Lemma A1 ensures that Ω_j is the unique state that holds in w. $\blacksquare$

In the following definition we adapt the well know notion of *zigzag connection* between Kripke models to our case of typed branching temporal logic (with next time operators) (*see* van Benthem [1]).

A3. DEFINITION: Let

$$\mathcal{M} = \langle \mathcal{M}_{t_1}, \ldots, \mathcal{M}_{t_n}, \mathcal{M}_G \rangle \quad \text{and} \quad \mathcal{M}' = \langle \mathcal{M}'_{t_1}, \ldots, \mathcal{M}'_{t_n}, \mathcal{M}'_G \rangle,$$

with $\mathcal{M}_t = \langle N_t, W_t, P_t \rangle$ and $\mathcal{M}'_t = \langle N'_t, W'_t, P'_t \rangle$ for $t \in \mathrm{TYP}$, be two models of $\mathbf{LGTT}_D$; the tuple $\langle C_{t_1}, \ldots, C_{t_n}, C_G \rangle$ is a *zigzag connection* between

$\mathcal{M}$ and $\mathcal{M}'$ iff for each type $t \in \mathrm{TYP}$ we have:

(i) $C_t \subseteq W_t \times W'_t$,

(ii) if $(w, w') \in C_t$ and $(w, v) \in N_t$ then $\exists v'$ s.t. $(w', v') \in N'_t$ and $(v, v') \in C_t$,

(iii) if $(w, w') \in C_t$ and $(w', v') \in N'_t$ then $\exists v$ s.t. $(w, v) \in N_t$ and $(v, v') \in C_t$,

(iv) if $(w, w') \in C_t$ then w and w' verify the same atomic formulas. ■

From this definition the next proposition follows immediately.

A4. PROPOSITION: *Let*

$$\mathcal{M} = \langle \mathcal{M}_{t_1}, \ldots, \mathcal{M}_{t_n}, \mathcal{M}_G \rangle \quad \text{and} \quad \mathcal{M}' = \langle \mathcal{M}'_{t_1}, \ldots, \mathcal{M}'_{t_n}, \mathcal{M}'_G \rangle,$$

with $\mathcal{M}_t = \langle N_t, W_t, P_t \rangle$ and $\mathcal{M}'_t = \langle N'_t, W'_t, P'_t \rangle$ for $t \in \mathrm{TYP}$, be two models of $\mathbf{LGTT}_D$; let $\langle C_{t\,1}, \ldots, C_{t_n}, C_G \rangle$ be a *zigzag connection* between $\mathcal{M}$ and $\mathcal{M}'$, then for each type $t \in \mathrm{TYP}$:

(i) if $(w, w') \in C_t$ and $b_w = \{w_i\}_{i<\omega}$ then

$$\exists\, b_{w'} = \{w'_i\}_{i<\omega} \text{ s.t.} \qquad \forall i \ (w_i, w'_i) \in C_t,$$

(ii) if $(w, w') \in C_t$ and $b_{w'} = \{w'_i\}_{i<\omega}$ then

$$\exists\, b_w = \{w_i\}_{i<\omega} \text{ s.t.} \qquad \forall i \ (w_i, w'_i) \in C_t. \quad \blacksquare$$

A5. PROPOSITION: *Let*

$$\mathcal{M} = \langle \mathcal{M}_{t_1}, \ldots, \mathcal{M}_{t_n}, \mathcal{M}_G \rangle \quad \text{and} \quad \mathcal{M}' = \langle \mathcal{M}'_{t_1}, \ldots, \mathcal{M}'_{t_n}, \mathcal{M}'_G \rangle,$$

with $\mathcal{M}_t = \langle N_t, W_t, P_t \rangle$ and $\mathcal{M}'_t = \langle N'_t, W'_t, P'_t \rangle$ for $t \in \mathrm{TYP}$, be two models of $\mathbf{LGTT}_D$ and let $\langle C_{t\,1}, \ldots, C_{t_n}, C_G \rangle$ be a *zigzag connection* between $\mathcal{M}$ and $\mathcal{M}'$, then for each type $t \in \mathrm{TYP}$, each wff_t α, and each $(w, w') \in C_t$ we have that $\mathcal{M}, w \underset{t}{\models} \alpha \Leftrightarrow \mathcal{M}', w' \underset{t}{\models} \alpha$.

Proof: The proof is done by structural induction on formulas:

1. if α is atomic, then $\mathcal{M}, w \underset{t}{\models} \alpha \Leftrightarrow \mathcal{M}', w' \underset{t}{\models} \alpha$ by definition of zigzag connection;

2. if $\alpha = \beta \supset \gamma$, then

$$\mathcal{M}, w \underset{t}{\models} \beta \supset \gamma$$

$$\Leftrightarrow \quad \text{(by induction hypothesis on } \beta \text{ and } \gamma) (\mathcal{M}, w \underset{t}{\models} \beta \Rightarrow \mathcal{M}, w \underset{t}{\models} \gamma)$$

$$\Leftrightarrow \quad (\mathcal{M}', w' \underset{t}{\models} \beta \Rightarrow \mathcal{M}', w' \underset{t}{\models} \gamma) \quad \Leftrightarrow \quad \mathcal{M}', w' \underset{t}{\models} \beta \supset \gamma;$$

3. if $\alpha = \neg \beta$, then

$$\mathscr{M}, w \underset{t}{\models} \neg \beta \Leftrightarrow \mathscr{M} \underset{t}{\not\models} \beta$$

$$\Leftrightarrow \text{(by induction hypothesis on } \beta) \; \mathscr{M}', w' \underset{t}{\not\models} \beta \Leftrightarrow \mathscr{M}', w' \underset{t}{\models} \neg \beta;$$

4. if $\alpha = EX\beta$, then

$$\mathscr{M}, w \underset{t}{\models} EX\beta \Leftrightarrow \exists w''(w, w'') \in NH\, \mathscr{M}, w'' \underset{t}{\models} \beta$$

$$\Leftrightarrow \text{(by induction hypothesis on } \beta)$$

and by definition of zigzag connection)

$$\exists w^{\wedge}(w', w^{\wedge}) \in NH'\, \mathscr{M}', w^{\wedge} \underset{t}{\models} \beta \Leftrightarrow \mathscr{M}', w' \underset{t}{\models} EX\beta;$$

5. if $\alpha = EF\beta$, then

$$\mathscr{M}, w \underset{t}{\models} EF\beta \Leftrightarrow \exists b_w \exists w'' \in b_w\, \mathscr{M}, w'' \underset{t}{\models} \beta$$

$$\Leftrightarrow \text{(by induction hypothesis on } \beta \text{ and by proposition A4)}$$

$$\exists b_{w'} \exists w^{\wedge} \in b_{w'}\, \mathscr{M}', w^{\wedge} \underset{t}{\models} \beta \Leftrightarrow \mathscr{M}', w' \underset{t}{\models} EF\beta;$$

6. if $\alpha = EG\beta$, then

$$\mathscr{M}, w \underset{t}{\models} EG\beta \Leftrightarrow \exists b_w \forall w'' \in b_w\, \mathscr{M}, w'' \underset{t}{\models} \beta$$

$$\Leftrightarrow \text{(by induction hypothesis on } \beta \text{ and by proposition A4)}$$

$$\exists b_{w'} \forall w^{\wedge} \in b_{w'}\, \mathscr{M}', w^{\wedge} \underset{t}{\models} \beta \Leftrightarrow \mathscr{M}', w' \underset{t}{\models} EG\beta. \quad \blacksquare$$

Now we will prove that each model of $\mathbf{LGTT}_D$ is zigzag connected with the syntatic model $\mathscr{H}_D^+$.

A5. PROPOSITION: *Let* $\mathscr{M} = \langle \mathscr{M}_{t_1}, \ldots, \mathscr{M}_{t_n}, \mathscr{M}_G \rangle$ *be a model of* $\mathbf{LGTT}_D$ *then there is a zigzag connection* $\langle C_{t_1}, \ldots, C_{t_n}, C_G \rangle$ *between* $\mathscr{M}$ *and* $\mathscr{H}_D^+$.

Proof: Let us fix a type t and the corresponding t-models

$$\mathscr{M}_t = \langle N_t, W_t, P_t \rangle \quad \text{and} \quad \mathscr{H}_t = \langle WH_t, NH_t, PH_t \rangle.$$

For each type t we define $C_t \subseteq W_t \times WH_t$ as the set of pairs (w, Ω) s. t. $\Omega = \Omega_w$ (*see* lemma A2). We have to verify that the relation C_t satisfies the condition

(ii), . . ., (iv) of definition A3. We have:

(ii) let us suppose $(w, \Omega) \in C_t$ and $(w, w') \in N_t$ and let us take $\Omega' = \Omega_{w'}$; in order to prove that $(\Omega, \Omega') \in NH_t$ let us suppose $(\Omega, \Omega') \notin NH_t$, this implies that $\Omega \supset EX\Omega'$ is not a theorem w. r. t. type t and therefore $\Omega \supset \neg EX\Omega'$ is a theorem w. r. t. type t; now, as $w \underset{t}{\models} \Omega$, we have that for each w' $(w, w') \in N_t$ implies that $w' \underset{t}{\models} \neg \Omega'$, that is a contradiction; moreover $(w', \Omega') \in C_t$ by our definition of C_t;

(iii) let us suppose $(w, \Omega) \in C_t$ and $(\Omega, \Omega') \in NH_t$; by definition of syntactic model we have that $\Omega \supset EX\Omega'$ is a theorem w. r. t. type t and therefore $w \underset{t}{\models} \Omega \supset EX\Omega'$; as $w \underset{t}{\models} \Omega$ there exists a world w' s.t. $(w, w') \in N_t$ and $w' \underset{t}{\models} \Omega'$ *i. e.* $\exists w'$ s. t. $(w, w') \in N_t$ and $(w, \Omega') \in C_t$;

(iv) let $(w, \Omega) \in C_t$ we have to prove that $w \underset{t}{\models} a$ iff $\Omega \underset{t}{\models} a$ for each atomic formula a of type t; we have two exhaustive cases: 1. $a \in \Omega$ and 2. $a \notin \Omega$; if case 1 holds then obviously $\Omega \underset{t}{\models} a$, and therefore as $w \underset{t}{\models} \Omega$ also $w \underset{t}{\models} a$; if case 2 holds then $\Omega \underset{t}{\not\models} a$; now we have the axiom $AG\neg(\Omega \wedge a)$, and therefore $w \underset{t}{\models} AG\neg(\Omega \wedge a)$ and, as $w \underset{t}{\models} \Omega$, we have $w \underset{t}{\not\models} a$. ■

Now we have all the tools to prove the following theorem.

A7. THEOREM: *For each* $D \in \mathcal{D}$, $\mathcal{H}_D^+$ *is the most general model,* i. e. *for* $t \in$ TYP, $\alpha \in wff_t$ *and for each model* $\mathcal{M}$, $\mathcal{H}_D^+ \underset{t}{\models} \alpha$ *implies* $\mathcal{M} \underset{t}{\models} \alpha$.

Proof: With respect to the type t let $\mathcal{M}_t = \langle W_t, N_t, P_t \rangle$ and $\mathcal{H}_t = \langle HS_t, HN_t, HP_t \rangle$ be the component of $\mathcal{M}$ and $\mathcal{H}_D^+$ respectively.

Let us suppose that $\mathcal{H}_D^+ \underset{t}{\models} \alpha$; we want to prove that $\mathcal{M} \underset{t}{\models} \alpha$; to do this let us prove that for a generic $w \in W_t$ we have $\mathcal{M}, w \underset{t}{\models} \alpha$. Let $w \in W_t$; using the zigzag connection C_t defined in proposition A6, we have that $(w, \Omega_w) \in C_t$ (where $\Omega_w \in WH_t$) and, by proposition A5, we have that for each $wff_t \beta$ $\mathcal{M}, w \underset{t}{\models} \beta \Leftrightarrow \mathcal{H}_D^+, \Omega_w \underset{t}{\models} \beta$. Now, by the hypothesis that $\mathcal{H}_D^+ \underset{t}{\models} \alpha$, we have that $\mathcal{H}_D^+, \Omega_w \underset{t}{\models} \alpha$ and therefore $\mathcal{M}, w \underset{t}{\models} \alpha$. ■