The Axiomatization of Propositional Linear Time Temporal Logic

Mariusz Giero
Institute of Sociology
University of Białystok
Poland

Summary. The article introduces propositional linear time temporal logic as a formal system. Axioms and rules of derivation are defined. Soundness Theorem and Deduction Theorem are proved [9].

MML identifier: LTLAXIO1, version: 7.11.07 4.160.1126

The terminology and notation used in this paper have been introduced in the following papers: [10], [3], [4], [5], [8], [11], [13], [1], [2], [6], [12], and [7].

1. Preliminaries

In this paper a, b, c denote boolean numbers.
Next we state three propositions:
(1) \((a \Rightarrow b \wedge c) \Rightarrow (a \Rightarrow b) = 1\).
(2) \((a \Rightarrow (b \Rightarrow c)) \Rightarrow (a \wedge b \Rightarrow c) = 1\).
(3) \((a \wedge b \Rightarrow c) \Rightarrow (a \Rightarrow (b \Rightarrow c)) = 1\).

2. The Language. Basic Operators. Further Operators as Abbreviations

We introduce the LTLB-WFF as a synonym of HP-WFF.
For simplicity, we adopt the following rules: \(p, q, r, s, A, B, C\) are elements of the LTLB-WFF, \(G\) is a subset of the LTLB-WFF, \(i, j, n\) are elements of \(\mathbb{N}\),
and \(f_1, f_2\) are finite sequences of elements of the LTLB-WFF.
We introduce $\bot$ as a synonym of VERUM.
Let us consider $p, q$. We introduce $p \mathcal{U} q$ as a synonym of $p \land q$.

We now state the proposition

(4) For every $A$ holds $A = \bot$ or there exists $n$ such that $A = \text{prop } n$ or there exist $p, q$ such that $A = p \Rightarrow q$ or there exist $p, q$ such that $A = p \mathcal{U} q$.

Let us consider $p$. The functor $\neg p$ yields an element of the LTLB-WFF and is defined as follows:

(Def. 1) $\neg p = p \Rightarrow \bot$.

The functor $\mathcal{X} p$ yielding an element of the LTLB-WFF is defined as follows:

(Def. 2) $\mathcal{X} p = \bot \mathcal{U} p$.

The element $\top$ of the LTLB-WFF is defined by:

(Def. 3) $\top = \neg \bot$.

Let us consider $p, q$. The functor $p \& q$ yields an element of the LTLB-WFF and is defined as follows:

(Def. 4) $p \& q = (p \Rightarrow (q \Rightarrow \bot)) \Rightarrow \bot$.

Let us consider $p, q$. The functor $p \| q$ yielding an element of the LTLB-WFF is defined as follows:

(Def. 5) $p \| q = \neg (p \& \neg q)$.

Let us consider $p$. The functor $\mathcal{G} p$ yielding an element of the LTLB-WFF is defined as follows:

(Def. 6) $\mathcal{G} p = \neg (p \| (\top \& (\top \mathcal{U} \neg p)))$.

Let us consider $p$. The functor $\mathcal{F} p$ yields an element of the LTLB-WFF and is defined as follows:

(Def. 7) $\mathcal{F} p = \neg \mathcal{G} \neg p$.

Let us consider $p, q$. The functor $p \mathcal{U} q$ yields an element of the LTLB-WFF and is defined as follows:

(Def. 8) $p \mathcal{U} q = q \| (p \& \neg (p \mathcal{U} q))$.

Let us consider $p, q$. The functor $p \mathcal{R} q$ yielding an element of the LTLB-WFF is defined as follows:

(Def. 9) $p \mathcal{R} q = \neg (p \mathcal{U} \neg q)$.

3. The Semantics

The subset $AP$ of the LTLB-WFF is defined by:

(Def. 10) For every set $x$ holds $x \in AP$ iff there exists an element $n$ of $\mathbb{N}$ such that $x = \text{prop } n$.

A LTL Model is a sequence of $2^{AP}$.

In the sequel $M$ denotes a LTL Model.
Let $M$ be a LTL Model. The functor $\text{SAT}_M$ yielding a function from $\mathbb{N} \times$ the LTLB-WFF into Boolean is defined by the condition (Def. 11).

(Def. 11) Let given $n$. Then

(i) $\text{SAT}_M(⟨n, \bot⟩) = 0,$

(ii) for every $k$ holds $\text{SAT}_M(⟨n, \text{prop } k⟩) = 1$ iff $\text{prop } k \in M(n),$ and

(iii) for all $p, q$ holds $\text{SAT}_M(⟨n, p \Rightarrow q⟩) = \text{SAT}_M(⟨n, p⟩) \Rightarrow \text{SAT}_M(⟨n, q⟩)$ and $\text{SAT}_M(⟨n, p U q⟩) = 1$ iff there exists $i$ such that $0 < i$ and $\text{SAT}_M(⟨n+i, q⟩) = 1$ and for every $j$ such that $1 \leq j < i$ holds $\text{SAT}_M(⟨n+j, p⟩) = 1.$

One can prove the following propositions:

(5) $\text{SAT}_M(⟨n, \neg A⟩) = 1$ iff $\text{SAT}_M(⟨n, A⟩) = 0.$

(6) $\text{SAT}_M(⟨n, T⟩) = 1.$

(7) $\text{SAT}_M(⟨n, A & B⟩) = 1$ iff $\text{SAT}_M(⟨n, A⟩) = 1$ and $\text{SAT}_M(⟨n, B⟩) = 1.$

(8) $\text{SAT}_M(⟨n, A | B⟩) = 1$ iff $\text{SAT}_M(⟨n, A⟩) = 1$ or $\text{SAT}_M(⟨n, B⟩) = 1.$

(9) $\text{SAT}_M(⟨n, X A⟩) = \text{SAT}_M(⟨n+1, A⟩).$

(10) $\text{SAT}_M(⟨n, G A⟩) = 1$ iff for every $i$ holds $\text{SAT}_M(⟨n+i, A⟩) = 1.$

(11) $\text{SAT}_M(⟨n, F A⟩) = 1$ if there exists $i$ such that $\text{SAT}_M(⟨n+i, A⟩) = 1.$

(12) $\text{SAT}_M(⟨n, p U q⟩) = 1$ if there exists $i$ such that $\text{SAT}_M(⟨n+i, q⟩) = 1$ and for every $j$ such that $j < i$ holds $\text{SAT}_M(⟨n+j, p⟩) = 1.$

(13) $\text{SAT}_M(⟨n, p R q⟩) = 1$ if and only if one of the following conditions is satisfied:

(i) there exists $i$ such that $\text{SAT}_M(⟨n+i, p⟩) = 1$ and for every $j$ such that $j \leq i$ holds $\text{SAT}_M(⟨n+j, q⟩) = 1,$ or

(ii) for every $i$ holds $\text{SAT}_M(⟨n+i, q⟩) = 1.$

(14) $\text{SAT}_M(⟨n, \neg X B⟩) = \text{SAT}_M(⟨n, X \neg B⟩).$

(15) $\text{SAT}_M(⟨n, \neg X B \Rightarrow \neg B⟩) = 1.$

(16) $\text{SAT}_M(⟨n, X \neg B \Rightarrow \neg X B⟩) = 1.$

(17) $\text{SAT}_M(⟨n, X(B \Rightarrow C) \Rightarrow (X B \Rightarrow X C)⟩) = 1.$

(18) $\text{SAT}_M(⟨n, G B \Rightarrow B & & G B⟩) = 1.$

(19) $\text{SAT}_M(⟨n, B U C \Rightarrow C \| X(B & & (B U C))⟩) = 1.$

(20) $\text{SAT}_M(⟨n, X C \| X(B & & (B U C)) \Rightarrow B U C⟩) = 1.$

(21) $\text{SAT}_M(⟨n, B U C \Rightarrow X F C⟩) = 1.$


Let us consider $M, p.$ The predicate $M \models p$ is defined as follows:

(Def. 12) For every element $n$ of $\mathbb{N}$ holds $\text{SAT}_M(⟨n, p⟩) = 1.$
Let us consider \( M, F \). The predicate \( M \models F \) is defined by:

(Def. 13) For every \( p \) such that \( p \in F \) holds \( M \models p \).

Let us consider \( F, p \). The predicate \( F \models p \) is defined as follows:

(Def. 14) For every \( M \) such that \( M \models F \) holds \( M \models p \).

One can prove the following propositions:

(22) \( M \models F \) and \( M \models G \) iff \( M \models F \cup G \).

(23) \( M \models A \) iff \( M \models \{ A \} \).

(24) If \( F \models A \) and \( F \models A \Rightarrow B \), then \( F \models B \).

(25) If \( F \models A \), then \( F \models \chi A \).

(26) If \( F \models A \), then \( F \models G A \).

(27) If \( F \models A \Rightarrow B \) and \( F \models A \Rightarrow \chi A \), then \( F \models A \Rightarrow G B \).

(28) SAT\(_{(M|1)}\)(\( \langle j, A \rangle \)) = SAT\(_{M}(\langle i + j, A \rangle)\).

(29) If \( F \models F \), then \( M \uparrow i \models F \).

(30) \( F \cup \{ A \} \models B \) iff \( F \models G A \Rightarrow B \).

Let \( f \) be a function from the LTLB-WFF into \( \text{Boolean} \). The functor \( \text{VAL}_f \) yielding a function from the LTLB-WFF into \( \text{Boolean} \) is defined as follows:

(Def. 15) \( (\text{VAL}_f)(\bot_i) = 0 \) and \( (\text{VAL}_f)(\text{prop} \; n) = f(\text{prop} \; n) \) and \( (\text{VAL}_f)(A \Rightarrow B) = (\text{VAL}_f)(A) \Rightarrow (\text{VAL}_f)(B) \) and \( (\text{VAL}_f)(A \cup B) = f(A \cup B) \).

The following propositions are true:

(31) For every function \( f \) from the LTLB-WFF into \( \text{Boolean} \) and for all \( p, q \) holds \( (\text{VAL}_f)(p \& \& q) = (\text{VAL}_f)(p) \land (\text{VAL}_f)(q) \).

(32) Let \( f \) be a function from the LTLB-WFF into \( \text{Boolean} \). Suppose that for every set \( B \) such that \( B \in \text{the LTLB-WFF} \) holds \( f(B) = \text{SAT}_M(\langle n, B \rangle) \).

Then \( (\text{VAL}_f)(A) = \text{SAT}_M(\langle n, A \rangle) \).

Let us consider \( p \). We say that \( p \) is tautologically valid if and only if:

(Def. 16) For every function \( f \) from the LTLB-WFF into \( \text{Boolean} \) holds \( (\text{VAL}_f)(p) = 1 \).

One can prove the following proposition

(33) If \( A \) is tautologically valid, then \( F \models A \).


Let \( D \) be a set. We say that \( D \) has LTL axioms if and only if the condition

(Def. 17) is satisfied.

(Def. 17) Let given \( p, q \). Then if \( p \) is tautologically valid, then \( p \in D \),

\[ \neg \chi p \Rightarrow \chi \neg p \in D, \]

\[ \chi \neg p \Rightarrow \neg \chi p \in D, \]
\[ \mathcal{X}(p \Rightarrow q) \Rightarrow (\mathcal{X} p \Rightarrow \mathcal{X} q) \in D, \]
\[ \mathcal{G} p \Rightarrow p \& \& \mathcal{X} \mathcal{G} p \in D, \]
\[ p \mathcal{U}_s q \Rightarrow \mathcal{X} q \parallel \mathcal{X}(p \& \&(p \mathcal{U}_s q)) \in D, \]
\[ \mathcal{X} q \parallel \mathcal{X}(p \& \&(p \mathcal{U}_s q)) \Rightarrow p \mathcal{U}_s q \in D, \]
\[ p \mathcal{U}_s q \Rightarrow \mathcal{X} \mathcal{F} q \in D. \]

The subset \( AX_{\text{LTL}} \) of the LTLB-WFF is defined as follows:

(Def. 18) \( AX_{\text{LTL}} \) has LTL axioms and for every subset \( D \) of the LTLB-WFF such that \( D \) has LTL axioms holds \( AX_{\text{LTL}} \subseteq D. \)

Let us mention that \( AX_{\text{LTL}} \) has LTL axioms.

Next we state two propositions:

(34) \( p \Rightarrow (q \Rightarrow p) \in AX_{\text{LTL}}. \)

(35) \( (p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r)) \in AX_{\text{LTL}}. \)

Let us consider \( p, q. \) The predicate \( \text{NEX}(p, q) \) is defined as follows:

(Def. 19) \( q = \mathcal{X} p. \)

Let us consider \( r. \) The predicate \( \text{MP}(p, q, r) \) is defined as follows:

(Def. 20) \( q = p \Rightarrow r. \)

The predicate \( \text{IND}(p, q, r) \) is defined as follows:

(Def. 21) There exist \( A, B \) such that \( p = A \Rightarrow B \) and \( q = A \Rightarrow \mathcal{X} A \) and \( r = A \Rightarrow \mathcal{G} B. \)

Let us observe that \( AX_{\text{LTL}} \) is non empty.

Let us consider \( A. \) We say that \( A \) is LTL axiom 1 if and only if:

(Def. 22) There exists \( B \) such that \( A = \neg \mathcal{X} B \Rightarrow \mathcal{X} \neg B. \)

We say that \( A \) is LTL axiom 1a if and only if:

(Def. 23) There exists \( B \) such that \( A = \mathcal{X} \neg B \Rightarrow \neg \mathcal{X} B. \)

We say that \( A \) is LTL axiom 2 if and only if:

(Def. 24) There exist \( B, C \) such that \( A = \mathcal{X}(B \Rightarrow C) \Rightarrow (\mathcal{X} B \Rightarrow \mathcal{X} C). \)

We say that \( A \) is LTL axiom 3 if and only if:

(Def. 25) There exists \( B \) such that \( A = \mathcal{G} B \Rightarrow B \& \& \mathcal{X} \mathcal{G} B. \)

We say that \( A \) is LTL axiom 4 if and only if:

(Def. 26) There exist \( B, C \) such that \( A = B \mathcal{U}_s C \Rightarrow \mathcal{X} C \parallel \mathcal{X}(B \& \&(B \mathcal{U}_s C)). \)

We say that \( A \) is LTL axiom 5 if and only if:

(Def. 27) There exist \( B, C \) such that \( A = \mathcal{X} C \parallel \mathcal{X}(B \& \&(B \mathcal{U}_s C)) \Rightarrow B \mathcal{U}_s C. \)

We say that \( A \) is LTL axiom 6 if and only if:

(Def. 28) There exist \( B, C \) such that \( A = B \mathcal{U}_s C \Rightarrow \mathcal{X} \mathcal{F} C. \)

Next we state two propositions:

(36) Every element of \( AX_{\text{LTL}} \) is tautologically valid, or LTL axiom 1, or LTL axiom 1a, or LTL axiom 2, or LTL axiom 3, or LTL axiom 4, or LTL axiom 5, or LTL axiom 6.
Suppose that $A$ is LTL axiom 1, or LTL axiom 1a, or LTL axiom 2, or LTL axiom 3, or LTL axiom 4, or LTL axiom 5, or LTL axiom 6. Then $F \models A$.

Let $i$ be a natural number and let us consider $f, X$. The predicate $\text{prc}(f, X, i)$ is defined by the conditions (Def. 29).

(Def. 29)(i) $f(i) \in AX_{LTL}$, or
(ii) $f(i) \in X$, or
(iii) there exist natural numbers $j, k$ such that $1 \leq j < i$ and $1 \leq k < i$ and MP($f_j, f_k, f_i$) or IND($f_j, f_k, f_i$), or
(iv) there exists a natural number $j$ such that $1 \leq j < i$ and NEX($f_j, f_i$).

Let us consider $X, p$. The predicate $X \models p$ is defined as follows:

(Def. 30) There exists $f$ such that $f(\text{len } f) = p$ and $1 \leq \text{len } f$ holds $\text{prc}(f, X, i)$.

We now state four propositions:

(38) Let $i, n$ be natural numbers. Suppose $n + \text{len } f \leq \text{len } f_2$ and for every natural number $k$ such that $1 \leq k \leq \text{len } f$ holds $f(k) = f_2(k + n)$ and $1 \leq i \leq \text{len } f$. If $\text{prc}(f, X, i)$, then $\text{prc}(f_2, X, i + n)$.

(39) Suppose that
(i) $f_2 = f \land f_1$,
(ii) $1 \leq \text{len } f$,
(iii) $1 \leq \text{len } f_1$,
(iv) for every natural number $i$ such that $1 \leq i \leq \text{len } f$ holds $\text{prc}(f, X, i)$, and
(v) for every natural number $i$ such that $1 \leq i \leq \text{len } f_1$ holds $\text{prc}(f_1, X, i)$.

Let $i$ be a natural number. If $1 \leq i \leq \text{len } f_2$, then $\text{prc}(f_2, X, i)$.

(40) Suppose $f = f_1 \land \langle p \rangle$ and $1 \leq \text{len } f_1$ and for every natural number $i$ such that $1 \leq i \leq \text{len } f_1$ holds $\text{prc}(f_1, X, i)$ and $\text{prc}(f, X, \text{len } f)$. Then for every natural number $i$ such that $1 \leq i \leq \text{len } f$ holds $\text{prc}(f, X, i)$ and $X \models p$.

(41) If $F \vdash A$, then $F \models A$.

6. Derivation of Some Formulas. Deduction Theorem of LTL

We now state a number of propositions:

(42) If $p \in AX_{LTL}$ or $p \in X$, then $X \vdash p$.
(43) If $X \vdash p$ and $X \vdash p \Rightarrow q$, then $X \vdash q$.
(44) If $X \vdash p$, then $X \vdash \lozenge p$.
(45) If $X \vdash p \Rightarrow q$ and $X \vdash p \Rightarrow \lozenge p$, then $X \vdash p \Rightarrow \lozenge q$.
(46) If $X \vdash r \Rightarrow p \& \& q$, then $X \vdash r \Rightarrow p$ and $X \vdash r \Rightarrow q$.

1Soundness Theorem for LTL
(47) If $X \vdash p \Rightarrow q$ and $X \vdash q \Rightarrow r$, then $X \vdash p \Rightarrow r$.

(48) If $X \vdash p \Rightarrow (q \Rightarrow r)$, then $X \vdash p \& \& q \Rightarrow r$.

(49) If $X \vdash p \& \& q \Rightarrow r$, then $X \vdash p \Rightarrow (q \Rightarrow r)$.

(50) If $X \vdash p \& \& q \Rightarrow r$ and $X \vdash p \Rightarrow s$, then $X \vdash p \& \& q \Rightarrow s \& \& r$.

(51) If $X \vdash p \Rightarrow (q \Rightarrow r)$ and $X \vdash p \Rightarrow (r \Rightarrow s)$, then $X \vdash p \Rightarrow (q \Rightarrow s)$.

(52) If $X \vdash p \Rightarrow q$, then $X \vdash \neg q \Rightarrow \neg p$.

(53) $X \vdash X p \& \& X q \Rightarrow X(p \& \& q)$.

If $F \vdash p$, then $F \vdash G p$.

If $p \Rightarrow q \in F$, then $F \cup \{p\} \vdash G q$.

If $F \vdash q$, then $F \cup \{p\} \vdash q$.

If $F \vdash \{p\} \vdash q$, then $F \vdash G p \Rightarrow q$.

If $F \vdash \{p\} \vdash q$, then $F \cup \{p\} \vdash q$.

If $F \vdash G p \Rightarrow q$, then $F \cup \{p\} \vdash q$.

If $F \vdash G(p \Rightarrow q)$, then $(G p \Rightarrow G q)$.

**References**


Received November 20, 2010

---

2Deduction Theorem of LTL