FORMALIZED MATHEMATICS
Vol. 19, No. 2, Pages 113–119, 2011
DOI: 10.2478/v10037-011-0018-1

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.

ISSN 1426–2630(p), 1898-9934(e)

We introduce $\bot_t$ as a synonym of VERUM.

Let us consider p, q. We introduce $p\,\mathcal{U}_s\,q$ as a synonym of $p \wedge q$.

We now state the proposition

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

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

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

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

(Def. 2) $\mathcal{X}\,p = \bot_t\,\mathcal{U}_s\,p$.

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

(Def. 3) $\top_t = \neg\bot_t$.

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

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

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

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

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

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

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) $p\,\mathcal{U}\,q = q\,||(p\,\&\&(p\,\mathcal{U}_s\,q))$.

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

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

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 $x = \mathrm{prop}\,n$.

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 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) $\mathrm{SAT}_M(\langle n, \bot_t\rangle) = 0$,

(ii) for every k holds $\mathrm{SAT}_M(\langle n, \mathrm{prop}\,k\rangle) = 1$ iff $\mathrm{prop}\,k \in M(n)$, and

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

One can prove the following propositions:

(5) $\mathrm{SAT}_M(\langle n, \neg A\rangle) = 1$ iff $\mathrm{SAT}_M(\langle n, A\rangle) = 0$.

(6) $\mathrm{SAT}_M(\langle n, \top_t\rangle) = 1$.

(7) $\mathrm{SAT}_M(\langle n, A \mathbin{\&\&} B\rangle) = 1$ iff $\mathrm{SAT}_M(\langle n, A\rangle) = 1$ and $\mathrm{SAT}_M(\langle n, B\rangle) = 1$.

(8) $\mathrm{SAT}_M(\langle n, A \,||\, B\rangle) = 1$ iff $\mathrm{SAT}_M(\langle n, A\rangle) = 1$ or $\mathrm{SAT}_M(\langle n, B\rangle) = 1$.

(9) $\mathrm{SAT}_M(\langle n, \mathcal{X}\,A\rangle) = \mathrm{SAT}_M(\langle n + 1, A\rangle)$.

(10) $\mathrm{SAT}_M(\langle n, \mathcal{G}\,A\rangle) = 1$ iff for every i holds $\mathrm{SAT}_M(\langle n + i, A\rangle) = 1$.

(11) $\mathrm{SAT}_M(\langle n, \mathcal{F}\,A\rangle) = 1$ iff there exists i such that $\mathrm{SAT}_M(\langle n + i, A\rangle) = 1$.

(12) $\mathrm{SAT}_M(\langle n, p\,\mathcal{U}\,q\rangle) = 1$ iff there exists i such that $\mathrm{SAT}_M(\langle n + i, q\rangle) = 1$ and for every j such that $j < i$ holds $\mathrm{SAT}_M(\langle n + j, p\rangle) = 1$.

(13) $\mathrm{SAT}_M(\langle n, p\,\mathcal{R}\,q\rangle) = 1$ if and only if one of the following conditions is satisfied:

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

(ii) for every i holds $\mathrm{SAT}_M(\langle n + i, q\rangle) = 1$.

(14) $\mathrm{SAT}_M(\langle n, \neg\,\mathcal{X}\,B\rangle) = \mathrm{SAT}_M(\langle n, \mathcal{X}\,\neg B\rangle)$.

(15) $\mathrm{SAT}_M(\langle n, \neg\,\mathcal{X}\,B \Rightarrow \mathcal{X}\,\neg B\rangle) = 1$.

(16) $\mathrm{SAT}_M(\langle n, \mathcal{X}\,\neg B \Rightarrow \neg\,\mathcal{X}\,B\rangle) = 1$.

(17) $\mathrm{SAT}_M(\langle n, \mathcal{X}(B \Rightarrow C) \Rightarrow (\mathcal{X}\,B \Rightarrow \mathcal{X}\,C)\rangle) = 1$.

(18) $\mathrm{SAT}_M(\langle n, \mathcal{G}\,B \Rightarrow B \mathbin{\&\&} \mathcal{X}\,\mathcal{G}\,B\rangle) = 1$.

(19) $\mathrm{SAT}_M(\langle n, B\,\mathcal{U}_s\,C \Rightarrow \mathcal{X}\,C \,||\, \mathcal{X}(B \mathbin{\&\&} (B\,\mathcal{U}_s\,C))\rangle) = 1$.

(20) $\mathrm{SAT}_M(\langle n, \mathcal{X}\,C \,||\, \mathcal{X}(B \mathbin{\&\&} (B\,\mathcal{U}_s\,C)) \Rightarrow B\,\mathcal{U}_s\,C\rangle) = 1$.

(21) $\mathrm{SAT}_M(\langle n, B\,\mathcal{U}_s\,C \Rightarrow \mathcal{X}\,\mathcal{F}\,C\rangle) = 1$.

4. Validity. Consequence. Some Facts about the Semantical Notions

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

(Def. 12) For every element n of $\mathbb{N}$ holds $\mathrm{SAT}_M(\langle n, p\rangle) = 1$.

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 $F \models \mathcal{X}\, A$.

(26) If $F \models A$, then $F \models \mathcal{G}\, A$.

(27) If $F \models A \Rightarrow B$ and $F \models A \Rightarrow \mathcal{X}\, A$, then $F \models A \Rightarrow \mathcal{G}\, B$.

(28) $\mathrm{SAT}_{(M\uparrow i)}(\langle j,\, A\rangle) = \mathrm{SAT}_M(\langle i+j,\, A\rangle)$.

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

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

Let f be a function from the LTLB-WFF into *Boolean*. The functor $\mathrm{VAL}\, f$ yielding a function from the LTLB-WFF into *Boolean* is defined as follows:

(Def. 15) $(\mathrm{VAL}\, f)(\perp_t) = 0$ and $(\mathrm{VAL}\, f)(\mathrm{prop}\, n) = f(\mathrm{prop}\, n)$ and $(\mathrm{VAL}\, f)(A \Rightarrow B) = (\mathrm{VAL}\, f)(A) \Rightarrow (\mathrm{VAL}\, f)(B)$ and $(\mathrm{VAL}\, f)(A\, \mathcal{U}_s\, B) = f(A\, \mathcal{U}_s\, B)$.

The following propositions are true:

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

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

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 *Boolean* holds $(\mathrm{VAL}\, f)(p) = 1$.

One can prove the following proposition

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

5. Axioms. Derivation Rules. Derivability. Soundness Theorem for LTL

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 $p \in D$,
$\neg\, \mathcal{X}\, p \Rightarrow \mathcal{X}\, \neg p \in D$,
$\mathcal{X}\, \neg p \Rightarrow \neg\, \mathcal{X}\, p \in D$,

$\mathcal{X}(p \Rightarrow q) \Rightarrow (\mathcal{X}\, p \Rightarrow \mathcal{X}\, q) \in D$,
$\mathcal{G}\, p \Rightarrow p \,\&\&\, \mathcal{X}\,\mathcal{G}\, p \in D$,
$p\,\mathcal{U}_s\, q \Rightarrow \mathcal{X}\, q \,||\, \mathcal{X}(p \,\&\&(p\,\mathcal{U}_s\, q)) \in D$,
$\mathcal{X}\, q \,||\, \mathcal{X}(p \,\&\&(p\,\mathcal{U}_s\, q)) \Rightarrow p\,\mathcal{U}_s\, q \in D$,
$p\,\mathcal{U}_s\, q \Rightarrow \mathcal{X}\,\mathcal{F}\, q \in D$.

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

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

Let us mention that AX_{LTL} has LTL axioms.

Next we state two propositions:

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

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

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

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

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

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

The predicate $\mathrm{IND}(p, q, r)$ 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_{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 $A = B\,\mathcal{U}_s\, C \Rightarrow \mathcal{X}\, C \,||\, \mathcal{X}(B \,\&\&(B\,\mathcal{U}_s\, C))$.

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

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

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_{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.

(37) 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 $\mathrm{prc}(f, X, i)$ is defined by the conditions (Def. 29).

(Def. 29)(i) $f(i) \in AX_{\mathrm{LTL}}$, 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 $\mathrm{MP}(f_j, f_k, f_i)$ or $\mathrm{IND}(f_j, f_k, f_i)$, or

(iv) there exists a natural number j such that $1 \leq j < i$ and $\mathrm{NEX}(f_j, f_i)$.

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

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

We now state four propositions:

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

(39) Suppose that

(i) $f_2 = f \frown f_1$,

(ii) $1 \leq \mathrm{len}\, f$,

(iii) $1 \leq \mathrm{len}\, f_1$,

(iv) for every natural number i such that $1 \leq i \leq \mathrm{len}\, f$ holds $\mathrm{prc}(f, X, i)$, and

(v) for every natural number i such that $1 \leq i \leq \mathrm{len}\, f_1$ holds $\mathrm{prc}(f_1, X, i)$.

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

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

(41)[1] 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 $p \in AX_{\mathrm{LTL}}$ 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 $X \vdash \mathcal{X}\, p$.

(45) If $X \vdash p \Rightarrow q$ and $X \vdash p \Rightarrow \mathcal{X}\, p$, then $X \vdash p \Rightarrow \mathcal{G}\, q$.

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

[1]Soundness 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 $X \vdash r \Rightarrow s$, then $X \vdash p \Rightarrow (q \Rightarrow s)$.

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

(53) $X \vdash \mathcal{X}\, p \,\&\&\, \mathcal{X}\, q \Rightarrow \mathcal{X}(p \,\&\&\, q)$.

(54) If $F \vdash p$, then $F \vdash \mathcal{G}\, p$.

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

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

(57)[2] If $F \cup \{p\} \vdash q$, then $F \vdash \mathcal{G}\, p \Rightarrow q$.

(58) If $F \vdash p \Rightarrow q$, then $F \cup \{p\} \vdash q$.

(59) If $F \vdash \mathcal{G}\, p \Rightarrow q$, then $F \cup \{p\} \vdash q$.

(60) $F \vdash \mathcal{G}(p \Rightarrow q) \Rightarrow (\mathcal{G}\, p \Rightarrow \mathcal{G}\, q)$.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[6] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[7] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[8] Adam Grabowski. Hilbert positive propositional calculus. *Formalized Mathematics*, 8(**1**):69–72, 1999.
[9] Fred Kröger and Stephan Merz. *Temporal Logic and State Systems*. Springer-Verlag, 2008.
[10] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[11] Andrzej Trybulec. Defining by structural induction in the positive propositional language. *Formalized Mathematics*, 8(**1**):133–137, 1999.
[12] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[13] Edmund Woronowicz. Many–argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.

Received November 20, 2010

[2]Deduction Theorem of LTL