



SAPIENZA
UNIVERSITÀ DI ROMA

Title

Facoltà di Ingegneria dell'Informazione, Informatica e Statistica
Corso di Laurea Magistrale in Engineering in Computer Science

Candidate

Francesco Fuggitti
ID number 1735212

Thesis Advisor

Prof. Giuseppe De Giacomo

Academic Year 2017/2018

Thesis not yet defended

Title

Master's thesis. Sapienza – University of Rome

© 2018 Francesco Fuggitti. All rights reserved

This thesis has been typeset by L^AT_EX and the Sapthesis class.

Author's email: fuggitti.1735212@studenti.uniroma1.it

Contents

1	Introduction	1
1.1	Context	1
1.2	Problem	1
1.3	Objectives	1
1.4	Results	1
1.5	Structure	1
2	PLTL and LTL_f	3
2.1	Linear Temporal Logic (LTL)	3
2.1.1	Syntax	4
2.1.2	Semantics	4
2.1.3	Complexity	5
2.2	Linear Temporal Logic on Finite Traces (LTL_f)	5
2.2.1	Syntax	5
2.2.2	Semantics	6
2.2.3	Complexity	7
2.3	Past Linear Temporal Logic (PLTL)	7
2.3.1	Syntax	7
2.3.2	Semantics	8
2.3.3	Complexity and Expressiveness	9
2.4	LTL_f and PLTL translation to automata	9
2.4.1	∂ function for LTL_f	10
2.4.2	∂ function for PLTL	11
2.5	LTL_f /PLTL to FOL Encoding and MONA	11
2.5.1	LTL_f -to-FOL Encoding	11
2.5.2	PLTL-to-FOL Encoding	13
2.5.3	MONA and FOL-to-MONA Encoding	14
3	LTL_f2DFA	17
3.1	Introduction	17
3.2	Package Structure	18
3.2.1	Lexer.py	18
3.2.2	Parser.py	20

3.2.3	Translator.py	23
3.2.4	DotHandler.py	31
3.3	Comparison with FLLOAT	32
3.4	Discussion	34
4	Janus	35
5	DFAGame	37
6	Conclusions and Future Work	39
	Bibliography	41

Chapter 1

Introduction

Here the intro of the intro

1.1 Context

here the context of the thesis

1.2 Problem

what is the problem solved

1.3 Objectives

what are the objective of the thesis

1.4 Results

what are the results achieved

1.5 Structure

what is the structure of the thesis

Chapter 2

PLTL and LTL_f

This chapter will deal with the theoretical framework on which all topics present in the thesis are based. Initially, we will introduce the widely known Linear-Time Temporal Logic (LTL) and the Past Linear Time Temporal Logic (PLTL), focusing on their syntax and semantic. Secondly, we will talk about the concept of *Finite Trace* in these formal languages and how it changes them. Specifically, we will describe the Linear Time Temporal Logic over Finite Traces (LTL_f). Then, we will illustrate the theory behind the transformation of an LTL_f or PLTL formula to a Deterministic Finite State Automaton (DFA). Finally, we will describe the translation of an LTL_f or PLTL formula to the classic First-Order Logic formalism (FOL) and the translation of a FOL formula into a program that the MONA, a tool that translates formulas into a DFA, can manage. Some examples will be provided, but we will suppose the reader to be confident with classical logic and automata theory.

2.1 Linear Temporal Logic (LTL)

Temporal Logic formalisms are a set of formal languages designed for representing temporal information and reasoning about time within a logical framework (Goranko and Galton, 2015). Indeed, these logics are used when propositions have their truth value dependent on time.

In this scenario, we find the *Linear Temporal Logic* (LTL) which is a a very well known modal temporal logic with modalities referring to time. It was originally proposed in (Pnueli, 1977) as a specification language for concurrent programs. Consequently, LTL has been extensively used in Artificial Intelligence and Computer Science. For instance, it has been employed in planning, reasoning about actions, declarative process mining and verification of software/hardware systems.

2.1.1 Syntax

Given a set of propositional symbols \mathcal{P} , a valid LTL formula φ is defined as follows:

$$\varphi ::= a \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \bigcirc\varphi \mid \varphi_1 \mathcal{U} \varphi_2$$

where $a \in \mathcal{P}$. The unary operator \bigcirc (*next-time*) and the binary operator \mathcal{U} (*until*) are temporal operators and we use \top and \perp to denote *true* and *false* respectively. Moreover, all classical logic operators $\vee, \Rightarrow, \Leftrightarrow, \text{true}$ and *false* can be used. Intuitively, $\bigcirc\varphi$ says that φ is true at the *next* instant, $\varphi_1 \mathcal{U} \varphi_2$ says that at some future instant, φ_2 will hold and *until* that point φ_1 holds. We also define common abbreviations for some specific temporal formulas: *eventually* as $\Diamond\varphi \doteq \text{true} \mathcal{U} \varphi$, *always* as $\Box\varphi \doteq \neg\Diamond\neg\varphi$, *weak-next* as $\bullet\varphi \doteq \neg\bigcirc\neg\varphi$ and *release* as $\varphi_1 \mathcal{R} \varphi_2 \doteq \neg(\neg\varphi_1 \mathcal{U} \neg\varphi_2)$.

LTL allows to express a lot of interesting properties defined over time. In the Example 2.1 we show some of them.

Example 2.1. Interesting LTL patterns:

- *Safety*: $\Box\varphi$, which means *it is always true that property in φ will happen* or *φ will hold forever*. For instance, $\Box\neg(\text{reactorTemp} > 1000)$ (the temperature of the reactor must never exceed 1000).
- *Liveness*: $\Diamond\varphi$, which means *sooner or later φ will hold* or *something good will eventually happen*. For instance, $\Diamond\text{rich}$ (eventually I will become rich).
- *Response*: $\Box\Diamond\varphi$ which means *for every point in time, there is a point later where φ holds*.
- *Persistence*: $\Diamond\Box\varphi$, which means *there exists a point in the future such that from then on φ always holds*.
- *Strong fairness*: $\Box\Diamond\varphi_1 \Rightarrow \Box\Diamond\varphi_2$, *if something is attempted/requested infinitely often, then it will be successful/allocated infinitely often*. For instance, $\Box\Diamond\text{ready} \Rightarrow \Box\Diamond\text{run}$ (if a process is in ready state infinitely often, then it will be selected by the scheduler infinitely often).

2.1.2 Semantics

The semantics of the main operators of LTL over *infinite traces* are expressed as an ω -word over the alphabet $2^{\mathcal{P}}$. We give the following definitions:

Definition 2.1. Given an infinite trace π , we inductively define when an LTL formula φ is *true* at an instant i , in symbols $\pi, i \models \varphi$, as follows:

$$\pi, i \models a, \text{ for } a \in \mathcal{P} \text{ iff } a \in \pi(i)$$

$$\pi, i \models \neg\varphi \text{ iff } \pi, i \not\models \varphi$$

$$\pi, i \models \varphi_1 \wedge \varphi_2 \text{ iff } \pi, i \models \varphi_1 \wedge \pi, i \models \varphi_2$$

$$\pi, i \models O\varphi \text{ iff } \pi, i+1 \models \varphi$$

$$\pi, i \models \varphi_1 \mathcal{U} \varphi_2 \text{ iff } \exists j. (j \geq i) \wedge \pi, j \models \varphi_2 \wedge \forall k. (i \leq k < j) \Rightarrow \pi, k \models \varphi_1$$

Definition 2.2. An LTL formula φ is *true* in π , in notation $\pi \models \varphi$, if $\pi, 0 \models \varphi$. A formula φ is *satisfiable* if it is true in some π and is *valid* if it is true in every π . A formula φ_1 *logically implies* another formula φ_2 , in symbols $\varphi_1 \models \varphi_2$ iff $\forall \pi, \pi \models \varphi_1 \Rightarrow \pi \models \varphi_2$.

Notice that satisfiability, validity and logical implication are all mutually reducible one to each other.

Example 2.2. Validity and logical implication as satisfiability

- φ is valid iff $\neg\varphi$ is unsatisfiable.
- $\varphi_1 \models \varphi_2$ iff $\varphi_1 \wedge \neg\varphi_2$ is unsatisfiable.

2.1.3 Complexity

About LTL complexity, we can state the following fundamental theorem:

Theorem 2.1. (*Sistla and Clarke, 1985*) *Satisfiability, validity, and logical implication for LTL formulas are PSPACE-complete.*

2.2 Linear Temporal Logic on Finite Traces (LTL_f)

Linear Temporal Logic on Finite Traces (LTL_f) is the variant of LTL described in Section 2.1 interpreted over *finite traces* (De Giacomo and Vardi, 2013). Although it seems a little difference, in some cases, the interpretation of a formula over finite traces completely changes its meaning with respect to the one over infinite traces.

2.2.1 Syntax

The syntax of LTL_f is exactly the same of LTL. Indeed, LTL_f formulas are built from a set \mathcal{P} of propositional symbols and are closed under the boolean connectives, the unary temporal operator O (*next-time*) and the binary operator \mathcal{U} (*until*). Formulas can be defined as follows:

$$\varphi ::= a \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid O\varphi \mid \varphi_1 \mathcal{U} \varphi_2$$

where $a \in \mathcal{P}$. All usual logical operators such as $\vee, \Rightarrow, \Leftrightarrow, true$ and *false* are also used. Similarly to LTL, we can define the following common abbreviations for temporal operators:

$$\Diamond\varphi \doteq true \mathcal{U} \varphi \tag{2.1}$$

$$\Box\varphi \doteq \neg\Diamond\neg\varphi \quad (2.2)$$

$$\bullet\varphi \doteq \neg\bigcirc\neg\varphi \quad (2.3)$$

$$\varphi_1 \mathcal{R} \varphi_2 \doteq \neg(\neg\varphi_1 \mathcal{U} \neg\varphi_2) \quad (2.4)$$

$$Last \doteq \bullet false \quad (2.5)$$

$$End \doteq \Box false \quad (2.6)$$

Compared with LTL, in LTL_f there have been defined also 2.5 and 2.6 which denotes the last instance of the trace and that the trace is ended, respectively. As we have seen in Example 2.1 with LTL, now we will see in Example 2.3 how properties expressed in LTL_f have changed their meaning with the interpretation over finite traces.

Example 2.3. Interesting LTL_f patterns:

- *Safety*: $\Box\varphi$, which now means always *till the end of the trace* φ holds.
- *Liveness*: $\Diamond\varphi$, which now means eventually *before the end of the trace* φ holds.
- *Response*: $\Box\Diamond\varphi$, which means for any point in the trace there exist a point later in the trace where φ holds. This property, interpreted over finite traces, can be seen also as $\Diamond(Last \wedge \varphi)$ because $\Box\Diamond\varphi$ implies that the *last point in the trace satisfies* φ .
- *Persistence*: $\Diamond\Box\varphi$ means that there is a point in the trace such that from then on until the end of the trace φ holds. Also here the meaning can be seen as $\Diamond(Last \wedge \varphi)$ since $\Diamond\Box\varphi$ implies that at the last point of the trace $\Box\varphi$, and so φ , holds.

In other words, no direct nesting of *eventually* and *always* connectives is meaningful in LTL_f. However, indirect nesting of *eventually* and *always* connectives can still produce meaningful and interesting properties. One example could be $\Box(\psi \Rightarrow \Diamond\varphi)$, which stands for *always, before the end of the trace, if ψ holds then φ will eventually hold*.

2.2.2 Semantics

The semantics of LTL_f is given as LT_f-interpretations, namely interpretations over a *finite traces* denoting a finite sequence of consecutive instants of time. Formally, LT_f-interpretations are expressed as finite words π over the alphabet $2^{\mathcal{P}}$, i.e. as alphabet we have all the possible propositional interpretations of the propositional symbols in \mathcal{P} . We use the following notation. We denote the *length* of a trace π as $length(\pi)$. We denote the *positions*, i.e. instants, on the trace as $\pi(i)$ with $0 \leq i \leq last$ where $last = length(\pi) - 1$ is the last element of the trace. We denote by $\pi(i, j)$, the *segment* (i.e., the subword) of π , the trace $\pi' = \langle \pi(i), \pi(i+1), \dots, \pi(j) \rangle$, with $0 \leq i \leq j \leq last$. We now give the following definitions:

Definition 2.3. Given an LTL_f -interpretation π , we define when an LTL_f formula φ is *true* at position i (for $0 \leq i \leq last$), in symbols $\pi, i \models \varphi$, inductively as follows:

$$\begin{aligned} \pi, i &\models a, \text{ for } a \in \mathcal{P} \text{ iff } a \in \pi(i) \\ \pi, i &\models \neg\varphi \text{ iff } \pi, i \not\models \varphi \\ \pi, i &\models \varphi_1 \wedge \varphi_2 \text{ iff } \pi, i \models \varphi_1 \wedge \pi, i \models \varphi_2 \\ \pi, i &\models \bigcirc\varphi \text{ iff } i < last \wedge \pi, i+1 \models \varphi \end{aligned} \tag{2.7}$$

$$\pi, i \models \varphi_1 \mathcal{U} \varphi_2 \text{ iff } \exists j. (i \leq j \leq last) \wedge \pi, j \models \varphi_2 \wedge \forall k. (i \leq k < j) \Rightarrow \pi, k \models \varphi_1 \tag{2.8}$$

The Definition 2.3 is exactly the same Definition 2.1 seen for LTL except for 2.7 and 2.8 in which the only difference lies on the intervals bounded by the last element of the trace.

Definition 2.4. An LTL_f formula is *true* in π , in notation $\pi \models \varphi$, if $\pi, 0 \models \varphi$. A formula φ is *satisfiable* if it is true in some LTL_f -interpretation, and is *valid* if it is true in every LTL_f -interpretation. A formula φ_1 *logically implies* another formula φ_2 , in symbols $\varphi_1 \models \varphi_2$ iff for every LTL_f -interpretation π we have that $\pi \models \varphi_1$ implies $\pi \models \varphi_2$.

2.2.3 Complexity

About LTL_f complexity, we can state the following theorem:

Theorem 2.2. (*De Giacomo and Vardi, 2013*) *Satisfiability, validity and logical implication for LTL_f formulas are PSPACE-complete.*

About LTL_f expressiveness, we have that:

Theorem 2.3. (*De Giacomo and Vardi, 2013; Gabbay et al., 1997*) *LTL_f has exactly the same expressive power of FOL over finite ordered sequences.*

2.3 Past Linear Temporal Logic (PLTL)

So far we have seen LTL and LTL_f languages, over infinite and finite traces respectively, that look into the future events. On the contrary, now we describe the so called *Past Linear Temporal Logic* (PLTL) which is the counterpart of the LTL and LTL_f because it uses temporal modalities for referring to past events, instead of future ones.

2.3.1 Syntax

The syntax of PLTL is exactly the same of the one seen in Section 2.1.1 for LTL and in Section 2.2.1 for LTL_f except for past temporal operators that are the inverse of the future ones. As stated before, PLTL formulas are built on top from a set \mathcal{P} of propositional

symbols and are closed under the boolean connectives, the unary temporal operator \ominus (*previous-time*) and the binary operator \mathcal{S} (*since*). Formulas can be defined as follows:

$$\varphi ::= a \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \ominus\varphi \mid \varphi_1 \mathcal{S} \varphi_2$$

where $a \in \mathcal{P}$. All usual logical operators such as $\vee, \Rightarrow, \Leftrightarrow, \text{true}$ and *false* can be derived. Similarly to LTL and LTL_f, we define the following common abbreviations for temporal operator:

$$\Diamond\varphi \doteq \text{true} \mathcal{S} \varphi \quad (2.9)$$

$$\Box\varphi \doteq \neg\Diamond\neg\varphi \quad (2.10)$$

In particular, $\Diamond\varphi$ in 2.9 is called *once* while $\Box\varphi$ in 2.10 is known as *historically*. Furthermore, both temporal operators *previous-time*, *since* and the two common abbreviations *once*, *historically* just defined above could be seen also as the inverse operators of future operators in LTL/LTL_f:

$$\ominus\varphi \equiv \mathcal{O}^{-1}\varphi$$

$$\varphi_1 \mathcal{S} \varphi_2 \equiv \varphi_1 \mathcal{U}^{-1}\varphi_2$$

$$\Diamond\varphi \equiv \Diamond^{-1}\varphi$$

$$\Box\varphi \equiv \Box^{-1}\varphi$$

2.3.2 Semantics

As we did previously with LTL and then with LTL_f, here we define a semantics to PLTL. The first important thing to notice is that a PLTL formula could be only interpreted over *finite* traces. This is due to the fact that, no matter how long the trace is, there must be a starting point in the past. Formally, a trace π is a word over the alphabet $2^{\mathcal{P}}$ and as alphabet we have all possible propositional interpretations of the propositional symbols in \mathcal{P} . We can now give the following definitions:

Definition 2.5. Given a trace π , we inductively define when a PLTL formula φ is *true* at time i , in symbols $\pi, i \models \varphi$, as follows:

$$\begin{aligned} \pi, i &\models a, \text{ for } a \in \mathcal{P} \text{ iff } a \in \pi(i) \\ \pi, i &\models \neg\varphi \text{ iff } \pi, i \not\models \varphi \\ \pi, i &\models \varphi_1 \wedge \varphi_2 \text{ iff } \pi, i \models \varphi_1 \wedge \pi, i \models \varphi_2 \\ \pi, i &\models \ominus\varphi \text{ iff } i > 0 \wedge \pi, i-1 \models \varphi \\ \pi, i &\models \varphi_1 \mathcal{S} \varphi_2 \text{ iff } \exists j. (j \leq i) \wedge \pi, j \models \varphi_2 \wedge \forall k. (j < k \leq i) \Rightarrow \pi, k \models \varphi_1 \end{aligned}$$

The Definition 2.5 is quite similar to Definitions 2.1 and 2.3. The only difference lies on the position in time of instances, indeed, in this case, we go backward.

2.3.3 Complexity and Expressiveness

About PLTL complexity, we can state the following theorem:

Theorem 2.4. *Satisfiability, validity and logical implication for PLTL formulas are PSPACE-complete.*

About expressiveness of PLTL, we can state the following theorem:

Theorem 2.5. *PLTL has exactly the same expressive power of LTL_f .*

However, it is worth to say that the LTL_f formalism augmented with past temporal operators present in PLTL can be exponentially more succinct than LTL_f (with only future operators) (Markey, 2003). Indeed, having at the same time past and future temporal operators is really useful because, in general, expressions given in natural language use references to events occurred in the past. We give an example in the following.

Example 2.4. Succinctness of LTL_f with Past:

$$\Box(\text{grant} \Rightarrow \Diamond \text{request}) \quad (2.11)$$

$$\neg((\neg \text{request})\mathcal{U}(\text{grant} \wedge \neg \text{request})) \quad (2.12)$$

Both formulas mean *every grant is preceeded by a request*. The former (2.11) is in LTL_f with past modalities whereas the latter (2.12) is pure LTL_f . It is pretty evident that the 2.11 is less intricate than the one in 2.12.

Finally, this property of LTL_f augmented with past temporal operators is interesting, however it is out of the scope of this thesis.

2.4 LTL_f and PLTL translation to automata

Given an LTL_f /PLTL formula φ , we can build a deterministic finite state automaton (DFA) (Rabin and Scott, 1959) \mathcal{A}_φ that accepts the same finite traces that makes φ true. To achieve this, we proceed in two steps: first, we translate LTL_f and PLTL formulas into an (NFA) (De Giacomo and Vardi, 2015) following a simple direct algorithm; secondly, the obtained NFA can be converted into a DFA following the standard *determinization* procedure.

Now, we recall definitions of NFA and DFA:

Definition 2.6. An NFA is a tuple $\mathcal{A} = \langle \Sigma, Q, q_0, \delta, F \rangle$, where:

- Σ is the input alphabet;
- Q is the finite set of states;
- $q_0 \in Q$ is the initial state;
- $\delta \subseteq Q \times \Sigma \times Q$ is the transition relation;

- $F \subseteq Q$ is the set of final states;

Definition 2.7. A DFA is a NFA where δ is a function $\delta : Q \times \Sigma \rightarrow Q$

To denote the set of all traces over Σ accepted by \mathcal{A} we will use $\mathcal{L}(\mathcal{A})$ henceforth.

In the next subsections, we will provide some definitions and we will illustrate the algorithm for the translation also giving an example.

2.4.1 ∂ function for LTL_f

In order to build the NFA, we need to define an auxiliary function ∂ as follows:

Definition 2.8. The *delta function* ∂ for LTL_f formulas is a function that takes as input an (implicitly quoted) LTL_f formula φ (in negation normal form (NNF)¹) and a propositional interpretation Π for \mathcal{P} (including *Last*), and returns a positive boolean formula whose atoms are (implicitly quoted) φ subformulas. It is defined as follows:

$$\begin{aligned}
 \partial(A, \Pi) &= \begin{cases} true & \text{if } A \in \Pi \\ false & \text{if } A \notin \Pi \end{cases} \\
 \partial(\neg A, \Pi) &= \begin{cases} false & \text{if } A \in \Pi \\ true & \text{if } A \notin \Pi \end{cases} \\
 \partial(\varphi_1 \wedge \varphi_2, \Pi) &= \partial(\varphi_1, \Pi) \wedge \partial(\varphi_2, \Pi) \\
 \partial(\varphi_1 \vee \varphi_2, \Pi) &= \partial(\varphi_1, \Pi) \vee \partial(\varphi_2, \Pi) \\
 \partial(\odot \varphi, \Pi) &= \varphi \wedge \neg End \equiv \varphi \wedge \Diamond true \\
 \partial(\varphi_1 \mathcal{U} \varphi_2, \Pi) &= \partial(\varphi_2, \Pi) \vee (\partial(\varphi_1, \Pi) \wedge \partial(\odot(\varphi_1 \mathcal{U} \varphi_2), \Pi)) \\
 \partial(\bullet \varphi, \Pi) &= \varphi \vee End \equiv \varphi \vee \Box false \\
 \partial(\varphi_1 \mathcal{R} \varphi_2, \Pi) &= \partial(\varphi_2, \Pi) \wedge (\partial(\varphi_1, \Pi) \vee \partial(\bullet(\varphi_1 \mathcal{R} \varphi_2), \Pi))
 \end{aligned} \tag{2.13}$$

where *End* is defined as Equation 2.6. As a consequence of Definition 2.8 and from Equation 2.1 and 2.2, we can deduce that

$$\begin{aligned}
 \partial(\Diamond \varphi, \Pi) &= \partial(\varphi, \Pi) \vee \partial(\odot \Diamond \varphi, \Pi) \\
 \partial(\Box \varphi, \Pi) &= \partial(\varphi, \Pi) \wedge \partial(\bullet \Box \varphi, \Pi)
 \end{aligned}$$

¹A formula is in *negation normal form* if negation (\neg) occurs only in front of atoms.

Moreover, we define $\partial(\varphi, \epsilon)$ which is inductively defined as Equation 2.13, except for the following cases:

$$\begin{aligned}
 \partial(A, \epsilon) &= false \\
 \partial(\neg A, \epsilon) &= false \\
 \partial(\bigcirc \varphi, \epsilon) &= false \\
 \partial(\bullet \varphi, \epsilon) &= true \\
 \partial(\varphi_1 \mathcal{U} \varphi_2, \epsilon) &= false \\
 \partial(\varphi_1 \mathcal{R} \varphi_2, \epsilon) &= true
 \end{aligned} \tag{2.14}$$

Note that $\partial(\varphi, \epsilon)$ is always either *true* or *false*. It is worth to observe for future use that from Equation 2.14 we can say $\partial(\Diamond \varphi, \epsilon) = false$ and $\partial(\Box \varphi, \epsilon) = true$.

2.4.2 ∂ function for PLTL

2.5 LTL_f/PLTL to FOL Encoding and MONA

In this section, we will illustrate how to translate an LTL_f and a PLTL formula into *first-order logic* (FOL) over finite linear ordered sequences² (De Giacomo and Vardi, 2013; Zhu et al., 2018). Then, we will present the MONA tool with its syntax and we will explain the translation procedure from a FOL encoding to the MONA encoding.

2.5.1 LTL_f-to-FOL Encoding

In the following we deal with a first-order language augmented with monadic predicates *succ*, *<* and *=* plus two constants 0 and *last*. Afterwards, we focus our attention to *finite linear ordered FOL interpretations* under the form of $\mathcal{I} = (\Delta^I, \cdot^{\mathcal{I}})$, where the domain is $\Delta^I = \{0, \dots, n\}$ with $n \in \mathbb{N}$, and the interpretation function $\cdot^{\mathcal{I}}$ interprets binary predicates and constants as follows:

$$\begin{aligned}
 succ^{\mathcal{I}} &= \{(i, i+1) \mid i \in \{0, \dots, n-1\}\} \\
 <^{\mathcal{I}} &= \{(i, j) \mid i, j \in \{0, \dots, n\} \wedge i < j\} \\
 =^{\mathcal{I}} &= \{(i, i) \mid i \in \{0, \dots, n\}\} \\
 0^{\mathcal{I}} &= 0 \\
 last^{\mathcal{I}} &= n
 \end{aligned} \tag{2.15}$$

²More precisely *monadic first-order logic on finite linearly ordered domains*, sometimes denoted as FO[<].

Actually, all these operators can be derived from $<$ as follows:

$$\begin{aligned} succ(x, y) &\doteq x < y \wedge \neg \exists z. x < z < y \\ x = y &\doteq \forall z. x < z \equiv y < z \\ 0 &\doteq x \mid \neg \exists y. succ(y, x) \\ last &\doteq x \mid \neg \exists y. succ(x, y) \end{aligned}$$

Although there could be possible differences in notation, the relation between LTL_f-interpretations and finite linear ordered FOL interpretations is isomorphic. Indeed, given an LTL_f-interpretation π we can define the corresponding FOL interpretation $\mathcal{I} = (\Delta^{\mathcal{I}}, \cdot^{\mathcal{I}})$ as follows: $\Delta^{\mathcal{I}} = \{0, \dots, last\}$, with $last = length(\pi) - 1$, with the predefined predicates and constants interpretation and, for each $a \in \mathcal{P}$ its interpretation is $a^{\mathcal{I}} = \{i \mid a \in \pi(i)\}$. On the contrary, given a finite linear ordered FOL interpretation $\mathcal{I} = (\Delta^{\mathcal{I}}, \cdot^{\mathcal{I}})$, with $\Delta^{\mathcal{I}} = \{0, \dots, n\}$, we determine the corresponding LTL_f-interpretation π as follows: $length(\pi) = n + 1$, for each instant $0 \leq i \leq last$ (with $last = n$), we obtain $\pi(i) = \{a \mid i \in a^{\mathcal{I}}\}$.

At this moment, we can define the translation function $fol(\varphi, x)$ in the following way.

Definition 2.9. Given an LTL_f formula φ and a variable x , the translation function $fol(\varphi, x)$, inductively defined on the LTL_f formula's structure, returns the corresponding FOL formula open in x :

$$\begin{aligned} fol(a, x) &= a(x) \\ fol(\neg \varphi, x) &= \neg fol(\varphi, x) \\ fol(\varphi_1 \wedge \varphi_2, x) &= fol(\varphi_1, x) \wedge fol(\varphi_2, x) \\ fol(\varphi_1 \vee \varphi_2, x) &= fol(\varphi_1, x) \vee fol(\varphi_2, x) \\ fol(\bigcirc \varphi, x) &= \exists y. succ(x, y) \wedge fol(\varphi, y) \\ fol(\bullet \varphi, x) &= x = last \vee \exists y. succ(x, y) \wedge fol(\varphi, y) \\ fol(\varphi_1 \mathcal{U} \varphi_2, x) &= \exists y. x \leq y \leq last \wedge fol(\varphi_2, y) \wedge \forall z. x \leq z < y \Rightarrow fol(\varphi_1, z) \\ fol(\varphi_1 \mathcal{R} \varphi_2, x) &= \exists y. x \leq y \leq last \wedge fol(\varphi_1, y) \wedge \forall z. x \leq z < y \Rightarrow fol(\varphi_2, z) \vee \\ &\quad \forall z. x \leq z < last \Rightarrow fol(\varphi_2, z) \end{aligned}$$

The following Theorem ensures that a finite trace ρ satisfies an LTL_f formula φ iff the corresponding finite linear ordered FOL interpretation \mathcal{I} of ρ models $fol(\varphi, 0)$.

Theorem 2.6. (*De Giacomo and Vardi, 2013*) Given an LTL_f-interpretation π and a corresponding finite linear ordered FOL interpretation \mathcal{I} , we have

$$\pi, i \models \varphi \text{ iff } \mathcal{I}, [x/i] \models fol(\varphi, x)$$

where $[x/i]$ stands for a variable assignments that assigns the value i to the free variable x of $fol(\varphi, x)$.

In general, recalling the Definition 2.4, a formula φ is *true* in a trace π ($\pi \models \varphi$) if $\pi, 0 \models \varphi$. Hence, we should evaluate our translation function $fol(\varphi, x)$ in 0 (i.e. computing $fol(\varphi, 0)$). Finally, since also the converse reduction of Theorem 2.6 holds, we can state the following Theorem:

Theorem 2.7. (*Gabbay et al., 1980*) LTL_f has exactly the same expressive power of FOL.

2.5.2 PLTL-to-FOL Encoding

As we have previously seen for LTL_f, in the current section we describe the translation function for a PLTL formula. Here, we also have a first-order language augmented with monadic predicates *prev*, $<$ and $=$ plus two constants 0 and *last*. Then, we have our *finite linear ordered FOL interpretations* under the form of $\mathcal{I} = (\Delta^I, \cdot^{\mathcal{I}})$, where the domain is $\Delta^I = \{0, \dots, n\}$ with $n \in \mathbb{N}$, and the interpretation function $\cdot^{\mathcal{I}}$ interprets the same binary predicates defined as 2.15 except that here we change *succ* with *prev* defined as follows:

$$prev^{\mathcal{I}} = \{(i, i-1) \mid i \in \{1, \dots, n\}\}$$

We can derive these operators from $<$ as well:

$$\begin{aligned} prev(x, y) &\doteq y < x \wedge \neg \exists z. y < z < x \\ x = y &\doteq \forall z. x < z \equiv y < z \\ 0 &\doteq x \mid \neg \exists y. prev(x, y) \\ last &\doteq x \mid \neg \exists y. prev(y, x) \end{aligned}$$

In the exactly same way done before, we can give the definition of the translation function $fol_p(\varphi, x)$:

Definition 2.10. Given a PLTL formula φ and a variable x , the translation function $fol_p(\varphi, x)$, inductively defined on the PLTL formula's structure, returns the corresponding FOL formula open in x :

$$\begin{aligned} fol_p(a, x) &= a(x) \\ fol_p(\neg \varphi, x) &= \neg fol_p(\varphi, x) \\ fol_p(\varphi_1 \wedge \varphi_2, x) &= fol_p(\varphi_1, x) \wedge fol_p(\varphi_2, x) \\ fol_p(\varphi_1 \vee \varphi_2, x) &= fol_p(\varphi_1, x) \vee fol_p(\varphi_2, x) \\ fol_p(\ominus \varphi, x) &= \exists y. prev(x, y) \wedge y \geq 0 \wedge fol_p(\varphi, y) \\ fol_p(\varphi_1 \mathcal{S} \varphi_2, x) &= \exists y. 0 \leq y \leq last \wedge fol_p(\varphi_2, y) \wedge \forall z. y < z \leq x \Rightarrow fol_p(\varphi_1, z) \end{aligned}$$

Consider a finite trace ρ , the corresponding FOL interpretation \mathcal{I} is defined as in Section 2.5.1. The following Theorem ensures that a finite trace ρ satisfies an PLTL formula φ iff the corresponding finite linear ordered FOL interpretation \mathcal{I} of ρ models $fol_p(\varphi, last)$.

Theorem 2.8. (*Kamp, 1968*) *Given a PLTL formula φ , a finite trace ρ , and the corresponding interpretation \mathcal{I} of ρ , we have that*

$$\rho \models \varphi \text{ iff } \mathcal{I} \models fol_p(\varphi, last)$$

where $last = length(\rho) - 1$.

2.5.3 MONA and FOL-to-MONA Encoding

In the following, firstly we introduce the MONA tool highlighting its main features, how it works and what is its role in this thesis. Secondly, we concentrate on the MONA syntax and we describe the algorithm to translate a FOL formula into a MONA program.

MONA

MONA (Elgaard et al., 1998) is a sophisticated tool written in C++ for the construction of symbolic DFA from logical specifications. This tool has been implemented starting from 1997 from the BRICS (a research center in computer science located at the Aarhus University) with the aim of efficiently implementing decision procedures for the *Weak Second-order Theory of One or Two successors* (ws1s/ws2s). These two theories are also called monadic (from here the name of the tool) second-order logics and are decidable³ since allowed second-order variables are interpreted as a finite set of numbers. Moreover, the ws1s theory is a fragment of arithmetic augmented with second-order quantification over finite sets of natural numbers. Indeed, first-order terms represents just natural numbers. Furthermore, ws1s has not the addition operator because that would make the theory undecidable, however there is the unary predicate $+1$ that stands for the successor function. On the other hand, ws2s is a generalization of ws1s to tree structures. Hence, MONA efficiently translates ws1s and ws2s formulas respectively into minimum DFAs and GTAs (Guided Tree Automata (Biehl et al., 1996)), representing them by shared, multi-terminal BDDs (Binary Decision Diagrams (Henriksen et al., 1995)). Having considered the polyedric features of MONA, we will only use the translation to DFAs.

MONA has a lot of possible applications that have been published during the years. Additionally, thanks to its APIs, it could be used both as a standalone tool and as an integrated tool for other programs. Some examples of MONA usage are the following:

- Hardware verification
- Controller systems

³A logic is decidable if there exists an algorithm such that for any given formula it determines its truth value.

- Program and Protocol verification
- Software Engineering

At this point, we can explain how MONA works, at least for the part related to the DFA construction from a FOL formula. However, before doing that, we would like to clarify what the exact role of MONA is within this thesis. As stated before and as we will see in Chapter 3, MONA has been employed as a tool that translates a monadic FOL formula on finite linearly ordered domains, encoded as a M2L-Str⁴, into a minimum DFA.

Now, we can briefly describe how MONA works.

FOL-to-MONA Encoding

The MONA syntax is quite similar to the WS1S syntax, but it has its own method to define variables and it has been enhanced with some special details, also known as syntactic sugar, making the overall language more readable and allowing to express things more clearly and more concisely.

⁴M2L-Str is a slight variation of WS1S where formulas are interpreted over *finite string* models, rather than *infinite string* models

Chapter 3

LTL_f2DFA

In this chapter we will present [LTL_f2DFA](#), a software package written in Python.

3.1 Introduction

LTL_f2DFA is a Python tool that processes a given LTL_f formula (with past and future operators) and generates the corresponding minimized DFA using MONA ([Elgaard et al., 1998](#)). In addition, it offers the possibility to compute the DFA with or without the DECLARE assumption ([De Giacomo et al., 2014](#)). The main features provided by the library are:

- parsing an LTL_f formula with past or future operators;
- translation of an LTL_f formula to MONA program;
- conversion of an LTL_f formula to DFA automaton.

LTL_f2DFA can be used with Python ≥ 3.6 and has the following dependencies:

- [PLY](#), a pure-Python implementation of the popular compiler construction tools [Lex and Yacc](#). It has been employed for parsing the input LTL_f formula;
- [MONA](#), a C++ tool that translates formulas to DFA. It has been used for the generation of the DFA;
- [Dotpy](#), a Python library able to parse and modify `.dot` files. It has been utilized for post-processing the MONA output.

The package is available to download on [PyPI](#) and you can install it by typing in the terminal:

```
pip install ltlf2dfa
```

All the code is available online on GitHub^{[1](#)}, it is open source and it is released under the [MIT License](#). Moreover, LTL_f2DFA can also be tried online at ltlf2dfa.diag.uniroma1.it.

¹<https://github.com/Francesco17/LTLf2DFA>

3.2 Package Structure

The structure of the LTL_f2DFA package is quite simple. It consists of a main folder called `ltlf2dfa/` which hosts the most important library's modules:

- `Lexer.py`, where the `Lexer` class is defined;
- `Parser.py`, where the `Parser` class is defined;
- `Translator.py`, where the main APIs for the translation are defined;
- `DotHandler.py`, where the MONA output is post-processed.

In the following paragraphs we will explore each module in detail.

3.2.1 `Lexer.py`

In the `Lexer.py` module we can find the declaration of the `MyLexer` class which is in charge of handling the input string and tokenizing it. Indeed, it implements a tokenizer that splits the input string into declared individual tokens. To our extent, we have defined the class as in Listing 3.1

Listing 3.1. `Lexer.py` module

```

1 import ply.lex as lex
2
3 class MyLexer(object):
4
5     reserved = {
6         'true':      'TRUE',
7         'false':     'FALSE',
8         'X':         'NEXT',
9         'W':         'WEAKNEXT',
10        'R':         'RELEASE',
11        'U':         'UNTIL',
12        'F':         'EVENTUALLY',
13        'G':         'GLOBALLY',
14        'Y':         'PASTNEXT', #PREVIOUS
15        'S':         'PASTUNTIL', #SINCE
16        'O':         'PASTEVENTUALLY', #ONCE
17        'H':         'PASTGLOBALLY' #HISTORICALLY
18    }
19    # List of token names. This is always required
20    tokens = (
21        'TERM',
22        'NOT',
23        'AND',

```

```

24         'OR',
25         'IMPLIES',
26         'DIMPLIES',
27         'LPAR',
28         'RPAR'
29     ) + tuple(reserved.values())
30
31     # Regular expression rules for simple tokens
32     t_TRUE = r'true'
33     t_FALSE = r'false'
34     t_AND = r'\&'
35     t_OR = r'\|'
36     t_IMPLIES = r'\->'
37     t_DIMPLIES = r'\<->'
38     t_NOT = r'\~'
39     t_LPAR = r'\('
40     t_RPAR = r'\)'
41     # FUTURE OPERATORS
42     t_NEXT = r'X'
43     t_WEAKNEXT = r'W'
44     t_RELEASE = r'R'
45     t_UNTIL = r'U'
46     t_EVENTUALLY = r'F'
47     t_GLOBALLY = r'G'
48     # PAST OPERATOR
49     t_PASTNEXT = r'Y'
50     t_PASTUNTIL = r'S'
51     t_PASTEVENTUALLY = r'O'
52     t_PASTGLOBALLY = r'H'
53
54     t_ignore = r'\n+'
55
56     def t_TERM(self, t):
57         r'(?![a-z])(?!true|false)[a-z]+'
58         t.type = MyLexer.reserved.get(t.value, 'TERM')
59         return t # Check for reserved words
60
61     def t_error(self, t):
62         print("Illegal character '%s' in the input formula" % t.value[0])
63         t.lexer.skip(1)
64
65     # Build the lexer
66     def build(self, **kwargs):

```

67

```
self.lexer = lex.lex(module=self, **kwargs)
```

Firstly, we have defined the reserved words within a dictionary so to match each reserved word with its identifier. Secondly, we have defined the tokens list with all possible tokens that can be produced by the lexer. This tokens list is always required for the implementation of a lexer. Then, each token has to be specified by writing a regular expression rule. If the token is simple it can be specified using only a string. Otherwise, for non trivial tokens we have to write the regular expression in a class method as for our token `TERM` in line 56. In that case, defining the token rule as a method is also useful when we would like to perform other actions. After that, we have a method to handle unrecognized tokens and, finally, we have written the function that builds the lexer.

3.2.2 Parser.py

In the `Parser.py` module we can find the declaration of `MyParser` class which implements the parsing component of PLY. The `MyParser` class operates after the `Lexer` has split the input string into known tokens. The main feature of the parser is to interpret and build the appropriate data structure for the given input. To this extent, the most important aspect of a parser is the definition of the *syntax*, usually specified in terms of a BNF² grammar, that should be unambiguous. Furthermore, `Yacc`, the parsing component of PLY, implements a parsing technique known as LR-parsing or shift-reduce parsing. In particular, this parsing technique works on a bottom up fashion that tries to recognize the right-hand-side of various grammar rules. Whenever a valid right-hand-side is found in the input, the appropriate action code is triggered and the grammar symbols are replaced by the grammar symbol on the left-hand-side and so on until there is no more rule to apply. The parser implementation is shown in Listing 3.2

Listing 3.2. `Parser.py` module

```
1 import ply.yacc as yacc
2 from ltlf2dfa.Lexer import MyLexer
3
4 class MyParser(object):
5
6     def __init__(self):
7         self.lexer = MyLexer()
8         self.lexer.build()
9         self.tokens = self.lexer.tokens
10        self.parser = yacc.yacc(module=self)
11        self.precedence = (
12
13            ('nonassoc', 'LPAR', 'RPAR'),
14            ('left', 'AND', 'OR', 'IMPLIES', 'DIMPLIES', 'UNTIL', \
15             'RELEASE', 'PASTUNTIL'),
```

²The Backus–Naur form is a notation technique for context-free grammars.


```

16         ('right', 'NEXT', 'WEAKNEXT', 'EVENTUALLY', \
17         'GLOBALLY', 'PASTNEXT', 'PASTEVENTUALLY', 'PASTGLOBALLY'),
18         ('right', 'NOT')
19     )
20
21     def __call__(self, s, **kwargs):
22         return self.parser.parse(s, lexer=self.lexer.lexer)
23
24     def p_formula(self, p):
25         '''
26         formula : formula AND formula
27                 | formula OR formula
28                 | formula IMPLIES formula
29                 | formula DIMPLIES formula
30                 | formula UNTIL formula
31                 | formula RELEASE formula
32                 | formula PASTUNTIL formula
33                 | NEXT formula
34                 | WEAKNEXT formula
35                 | EVENTUALLY formula
36                 | GLOBALLY formula
37                 | PASTNEXT formula
38                 | PASTEVENTUALLY formula
39                 | PASTGLOBALLY formula
40                 | NOT formula
41                 | TRUE
42                 | FALSE
43                 | TERM
44         '''
45
46         if len(p) == 2: p[0] = p[1]
47         elif len(p) == 3:
48             if p[1] == 'F': # F(a) == true UNTIL A
49                 p[0] = ('U', 'true', p[2])
50             elif p[1] == 'G': # G(a) == not(eventually (not A))
51                 p[0] = ('~', ('U', 'true', ('~', p[2])))
52             elif p[1] == 'O': # O(a) = true SINCE A
53                 p[0] = ('S', 'true', p[2])
54             elif p[1] == 'H': # H(a) == not(pasteventually(not A))
55                 p[0] = ('~', ('S', 'true', ('~', p[2])))
56             elif p[1] == 'W':
57                 p[0] = ('~', ('X', ('~', p[2])))
58         else:

```

```

59         p[0] = (p[1], p[2])
60     elif len(p) == 4:
61         if p[2] == '>':
62             p[0] = ('|', ('~', p[1]), p[3])
63         elif p[2] == '<->':
64             p[0] = ('&', ('|', ('~', p[1]), p[3]), ('|', ('~', p[3]), \
65                 p[1]))
66         elif p[2] == 'R':
67             p[0] = ('~', ('U', ('~', p[1]), ('~', p[3])))
68         else:
69             p[0] = (p[2], p[1], p[3])
70     else: raise ValueError
71
72
73     def p_expr_group(self, p):
74         '''
75         formula : LPAR formula RPAR
76         '''
77         p[0] = p[2]
78
79     def p_error(self, p):
80         raise ValueError("Syntax error in input! %s" %str(p))

```

As we can see, as soon as the parser is instantiated it builds the lexer, gets the tokens and defines their precedence if needed. Then, we have defined methods of the `MyParser` class that are in charge of constructing the syntax tree structure from tokens found by the lexer in the input string. In our case, we have chosen to use as data structure a tuple of tuples as it is the one of the simplest data structure in Python. In general, a tuple of tuples represents a tree where each node represents an item present in the formula.

For instance, the LTL_f formula $\varphi = G(a \rightarrow Xb)$ is represented as $(\sim, (U, true, (\sim, (|, (\sim, a), (X, b))))))$ and it corresponds to a tree as the one depicted in Figure 3.1. Finally, as in the `MyLexer` class, we have to handle errors defining a specific method.

LTL_f 2DFA can be used just for the parsing phase of an LTL_f formula as shown in Listing 3.3.

Listing 3.3. How to use only the parsing phase of LTL_f 2DFA.

```

1 from ltlf2dfa.Parser import MyParser
2
3 formula = "G(a->Xb)"
4 parser = MyParser()
5 parsed_formula = parser(formula)
6
7 print(parsed_formula) # syntax tree as tuple of tuples

```

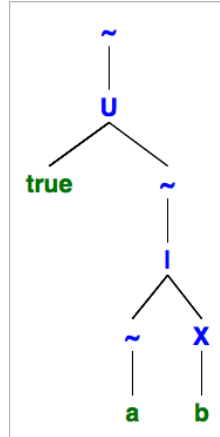


Figure 3.1. The syntax tree generated for the formula " $G(a \sim Xb)$ ". Symbols are in green while operators are in blue.

3.2.3 Translator.py

The `Translator.py` module contains the majority of APIs that the `LTLf2DFA` package exposes. Indeed, this module consists of a `Translator` class which concerns the core feature of the package: the translation of an `LTLf` formula into a DFA. Since the package takes advantage of the MONA tool for the formula conversion, the `Translator` class has to translate first the given formula into the syntax recognized by MONA, then create the input program for MONA and, finally, invoke MONA to get back the resulting DFA in the Graphviz³ format. The main methods of the `Translator` class are:

- `translate()`, which starting from the formula syntax tree generated (Figure 3.1) in the parsing phase translates it into a string using the syntax of MONA;
- `createMonafile(flag)`, which, as the name suggests, creates the program `.mona` that will be given as input to MONA. The flag parameter is going to be `True` or `False` whether we need to compute also DECLARE assumptions or not;
- `invoke_mona()`, which invokes MONA in order to obtain the DFA.

Now we will go into details of the methods stated above showing their implementation.

The `translate` method

The `translate` method is a crucial step towards reaching a good result and performance. Formally, the translation procedure from an `LTLf` formula to the MONA syntax is done passing through FOL as shown in 3.1.

$$\text{LTL}_f \rightarrow \text{FOL} \rightarrow \text{MONA} \quad (3.1)$$

³Graphviz is open source graph visualization software. For further details see [https://www. .org](https://www.graphviz.org)

The former translation from LTL_f to FOL is done accordingly to (De Giacomo and Vardi, 2013), while the latter follows from (Klarlund and Møller, 2001). In Listing 3.4 we can see the translation's implementation. Three dots ... represent omitted code.

Listing 3.4. The translate method.

```

1  import ...
2
3  class Translator:
4      ...
5
6      def translate(self):
7          self.translated_formula = translate_bis(self.parsed_formula, \
8              var='v_0')+";\n"
9
10     ...
11
12 def translate_bis(formula_tree, var):
13     if type(formula_tree) == tuple:
14         #enable this print to see the tree pruning
15         # print(self.parsed_formula)
16         # print(var)
17         if formula_tree[0] == '&':
18             # print('computed tree: ' + str(self.parsed_formula))
19             if var == 'v_0':
20                 a = translate_bis(formula_tree[1], '0')
21                 b = translate_bis(formula_tree[2], '0')
22             else:
23                 a = translate_bis(formula_tree[1], var)
24                 b = translate_bis(formula_tree[2], var)
25             if a == 'false' or b == 'false':
26                 return 'false'
27             elif a == 'true':
28                 if b == 'true': return 'true'
29                 else: return b
30             elif b == 'true': return a
31             else: return '('+a+'&'+b+')'
32         elif formula_tree[0] == '|':
33             # print('computed tree: ' + str(self.parsed_formula))
34             if var == 'v_0':
35                 a = translate_bis(formula_tree[1], '0')
36                 b = translate_bis(formula_tree[2], '0')
37             else:
38                 a = translate_bis(formula_tree[1], var)
39                 b = translate_bis(formula_tree[2], var)

```

```

40     if a == 'true' or b == 'true':
41         return 'true'
42     elif a == 'false':
43         if b == 'true': return 'true'
44         elif b == 'false': return 'false'
45         else: return b
46     elif b == 'false': return a
47     else: return '('+a+'|'+b+')'
48 elif formula_tree[0] == '~':
49     # print('computed tree: ' + str(self.parsed_formula))
50     if var == 'v_0': a = translate_bis(formula_tree[1], '0')
51     else: a = translate_bis(formula_tree[1], var)
52     if a == 'true': return 'false'
53     elif a == 'false': return 'true'
54     else: return '~('+ a +')'
55 elif formula_tree[0] == 'X':
56     # print('computed tree: ' + str(self.parsed_formula))
57     new_var = _next(var)
58     a = translate_bis(formula_tree[1],new_var)
59     if var == 'v_0':
60         return '('+ 'ex1'+new_var+':'+ new_var +'_=1'+ '&'+ \
61             a +')'
62     else:
63         return '('+ 'ex1'+new_var+':'+ new_var +'_=' + var + \
64             '+1'+ '&'+ a +')'
65 elif formula_tree[0] == 'U':
66     # print('computed tree: ' + str(self.parsed_formula))
67     new_var = _next(var)
68     new_new_var = _next(new_var)
69     a = translate_bis(formula_tree[2],new_var)
70     b = translate_bis(formula_tree[1],new_new_var)
71
72     if var == 'v_0':
73         if b == 'true': return '('+ 'ex1'+new_var+':0<=' + \
74             new_var+ '&'+ new_var+ '<=max($)&'+ a +')'
75         elif a == 'true': return '('+ 'ex1'+new_var+':0<=' + \
76             new_var+ '&'+ new_var+ '<=max($)&all1'+ \
77             new_new_var+':0<=' + new_new_var+ '&'+ \
78             new_new_var+ '<'+ new_var+ '>'+ b +')'
79         elif a == 'false': return 'false'
80         else: return '('+ 'ex1'+new_var+':0<=' + new_var+ \
81             '&'+ new_var+ '<=max($)&'+ a + '&all1'+ \
82             new_new_var+':0<=' + new_new_var+ '&'+ \

```

```

83     new_new_var+'_<_' + new_var+'_>_' + b+'_')'
84 else:
85     if b == 'true': return '(' + 'ex1_' + new_var+'_' + var + \
86         '_<_' + new_var+'_' + new_var+'_<=max($)' + a + '_' + ')'
87     elif a == 'true': return '(' + 'ex1_' + new_var+'_' + var + \
88         '_<_' + new_var+'_' + new_var+'_<=max($)' + all1_' + \
89         new_new_var+'_' + var+'_<_' + new_new_var+'_' + \
90         new_new_var+'_<_' + new_var+'_>_' + b+'_')'
91     elif a == 'false': return 'false'
92     else: return '(' + 'ex1_' + new_var+'_' + var+'_<=_' + \
93         new_var+'_' + new_var+'_<=max($)' + a + \
94         '_&all1_' + new_new_var+'_' + var+'_<_' + new_new_var+'_' + \
95         '_&_' + new_new_var+'_<_' + new_var+'_>_' + b+'_')'
96 elif formula_tree[0] == 'Y':
97     # print('computed tree: ' + str(self.parsed_formula))
98     new_var = _next(var)
99     a = translate_bis(formula_tree[1], new_var)
100    if var == 'v_0':
101        return '(' + 'ex1_' + new_var+'_' + new_var + \
102            '_<=max($)' + all1_' + '&max($)' + '>0' + a + ')'
103    else:
104        return '(' + 'ex1_' + new_var+'_' + new_var + \
105            '_<_' + var + '_<1_' + '&_' + new_var+'_>0' + a + ')'
106 elif formula_tree[0] == 'S':
107     # print('computed tree: ' + str(self.parsed_formula))
108     new_var = _next(var)
109     new_new_var = _next(new_var)
110     a = translate_bis(formula_tree[2], new_var)
111     b = translate_bis(formula_tree[1], new_new_var)
112
113    if var == 'v_0':
114        if b == 'true': return '(' + 'ex1_' + new_var+'_' + '0' + '<=_' + \
115            new_var+'_' + new_var+'_<=max($)' + a + '_' + ')'
116        elif a == 'true': return '(' + 'ex1_' + new_var+'_' + \
117            '0' + '<=_' + new_var+'_' + new_var+'_' + \
118            '_<=max($)' + all1_' + new_new_var+'_' + new_var+'_<_' + \
119            new_new_var+'_' + new_new_var+'_<=max($)' + '>_' + b+'_')'
120        elif a == 'false': return 'false'
121        else: return '(' + 'ex1_' + new_var+'_' + '0' + '<=_' + \
122            new_var+'_' + new_var+'_<=max($)' + a + \
123            '_&all1_' + new_new_var+'_' + new_var+'_<_' + \
124            new_new_var+'_' + new_new_var+'_<=max($)' + '>_' + b+'_')'
125    else:

```

```

126         if b == 'true': return '('+ 'ex1'+new_var+ \
127             ':_0_<=_'+new_var+'_&_'+new_var+'_<=_max($)_&_'+ a +'_)\'
128         elif a == 'true': return '('+ 'ex1'+new_var+ \
129             ':_0_<=_'+new_var+'_&_'+new_var+'_<=_'+var+ \
130             '_&_all1'+new_new_var+':_'+new_var+'_<_'+ \
131             new_new_var+'_&_'+new_new_var+'_<=_'+var+'_>_'+b+')\'
132         elif a == 'false': return 'false'
133         else: return '('+ 'ex1'+new_var+':_0_<=_'+ \
134             new_var+'_&_'+new_var+'_<=_'+var+'_&_'+ a +'_&_all1'+ \
135             new_new_var+':_'+new_var+'_<_'+new_new_var+'_&_'+ \
136             new_new_var+'_<=_'+var+'_>_'+b+')\'
137     else:
138         # handling non-tuple cases
139         if formula_tree == 'true': return 'true'
140         elif formula_tree == 'true': return 'false'
141
142         # enable if you want to see recursion
143         # print('computed tree: '+ str(self.parsed_formula))
144
145         # BASE CASE OF RECURSION
146     else:
147         if formula_tree.isalpha():
148             if var == 'v_0':
149                 return '_0_in_'+ formula_tree.upper()
150             else:
151                 return var + '_in_' + formula_tree.upper()
152         else:
153             return var + '_in_' + formula_tree
154
155 def _next(var):
156     if var == '0': return 'v_1'
157     else:
158         s = var.split('_')
159         s[1] = str(int(s[1])+1)
160         return '_'.join(s)

```

As we can see, the `translate` method is actually very simple. In fact, it just calls the `translate_bis` function (line 12) to perform the proper translation. The function works in a recursive fashion taking as input the parsed formula and a variable and outputting a string containing the result. Obviously, when an instance of the `Translator` class is created the input formula is checked to have either only future or past operators. The base case of the recursion handles the translation of symbols as they are the leaves of the syntax tree composed in the parsing phase (Figure 3.1). On the other hand, the recursive step regards the handling of operators (non leaf components of the syntax

tree) which are in our case $\wedge, \vee, \neg, \bigcirc, \mathcal{U}, \ominus, \mathcal{S}$. During the translation, we simplify the resulting formula by avoiding pieces of the expression that are logically **True** or **False**. This simplification has two main advantages. First, it substantially reduces the length of the resulting formula, improving its readability. Second, it increases the computation performances of MONA. Additionally, since the MONA syntax requires the declaration of the free variables, the `translate_bis` function has to compute also the appropriate free variables declaration. In this terms, the translation function uses the `_next` function to compute the next variable each time is needed.

The `createMonafile` method

The `createMonafile` method is employed to write the program `.mona` and save it in the main directory. It takes as input a boolean flag that, as stated before, stands for indicating whether one would like to compute and add the **DECLARE** assumption or not. In particular, in formal logic, as stated in (De Giacomo et al., 2014), the **DECLARE** assumption is expressed as in 3.2.

$$\Box(\bigvee_{a \in \mathcal{P}} a) \wedge \Box(\bigwedge_{a, b \in \mathcal{P}, a \neq b} a \rightarrow \neg b) \quad (3.2)$$

It consists essentially in two parts joined by the \wedge operator. The former indicates that it is always true that at each point in time only one symbol is *true*, while the latter means that always for each couple of different symbols in the formula if one is *true* the other must be *false*. The practical part can be seen in Listing 3.5.

Listing 3.5. The `createMonafile` method.

```

1  ...
2  def compute_declare_assumption(self):
3      pairs = list(it.combinations(self.alphabet, 2))
4
5      if pairs:
6          first_assumption = "~(ex1_␣y:␣0<=y_␣&_␣y<=max($)_␣&_␣~("
7          for symbol in self.alphabet:
8              if symbol == self.alphabet[-1]: first_assumption += \
9                  'y_␣in_␣'+ symbol +'))'
10             else : first_assumption += 'y_␣in_␣'+ symbol +'_␣|_␣'
11
12         second_assumption = "~(ex1_␣y:␣0<=y_␣&_␣y<=max($)_␣&_␣~("
13         for pair in pairs:
14             if pair == pairs[-1]: second_assumption += '(y_␣notin_␣'+ \
15                 pair[0]+'_␣|_␣y_␣notin_␣'+pair[1]+ ')))';
16             else: second_assumption += '(y_␣notin_␣'+ pair[0]+ \
17                 '_␣|_␣y_␣notin_␣'+pair[1]+ ')_␣&_␣'
18
19         return first_assumption +'_␣&_␣'+ second_assumption

```



```

20         else:
21             return None
22
23     def buildMonaProgram(self, flag_for_declare):
24         if not self.alphabet and not self.translated_formula:
25             raise ValueError
26         else:
27             if flag_for_declare:
28                 if self.compute_declare_assumption() is None:
29                     if self.alphabet:
30                         return self.headerMona + \
31                             'var2_' + ",".join(self.alphabet) + ';\n' + \
32                             self.translated_formula
33                     else:
34                         return self.headerMona + self.translated_formula
35             else: return self.headerMona + 'var2_' + \
36                 ",".join(self.alphabet) + ';\n' + \
37                 self.translated_formula + \
38                 self.compute_declare_assumption()
39         else:
40             if self.alphabet:
41                 return self.headerMona + 'var2_' + \
42                     ",".join(self.alphabet) + ';\n' + \
43                     self.translated_formula
44             else:
45                 return self.headerMona + self.translated_formula
46
47     def createMonafile(self, flag):
48         program = self.buildMonaProgram(flag)
49         try:
50             with open('./automa.mona', 'w+') as file:
51                 file.write(program)
52                 file.close()
53         except IOError:
54             print('Problem with the opening of the file!')
55     ...

```

As shown in the code, the `createMonafile` method calls another method, the `buildMonaProgram` (line 23), which literally builds the *.mona* program by joining all pieces that should belong to it. Instead, regarding the `DECLARE` assumption, if needed, it is added to the *.mona* program directly translated through `compute_declare_assumption` method at line 2.

The `invoke_mona` method

Finally, the `invoke_mona` method is the one that executes the MONA compiled executable giving it the `.mona` program. Consequently, the DFA resulting from the computation of MONA will be stored in the main directory. As stated in 3.1, the LTL_f2DFA package requires MONA to be installed. Indeed, without this requirements the `invoke_mona` method will raise an error. The implementation can be seen in Listing 3.6.

Listing 3.6. The `invoke_mona` method.

```

1  ...
2  def invoke_mona(self, path='./inter-automa'):
3      if sys.platform == 'linux':
4          package_dir = os.path.dirname(os.path.abspath(__file__))
5          mona_path = pkg_resources.resource_filename('ltlf2dfa', 'mona')
6          if os.access(mona_path, os.X_OK): #check if mona is executable
7              try:
8                  subprocess.call(package_dir+'./mona_u-gw' + \
9                                  './automa.mona>' + path + '.dot', shell=True)
10             except subprocess.CalledProcessError as e:
11                 print(e)
12                 exit()
13             except OSError as e:
14                 print(e)
15                 exit()
16         else:
17             print('[ERROR]: MONA tool is not executable...')
18             exit()
19     else:
20         try:
21             subprocess.call('mona_u-gw./automa.mona>' + path + \
22                             '.dot', shell=True)
23         except subprocess.CalledProcessError as e:
24             print(e)
25             exit()
26         except OSError as e:
27             print(e)
28             exit()
29  ...

```

To the execute of the MONA tool we have leveraged the built-in module `subprocess` that enables to spawn new processes, connect to their input/output/error pipes, and obtain their return codes.

Unfortunately, the DFA resulting from MONA needs to be post-processed because of some extra states added for other purposes not relevant for us. This aspect will be better explained in the following subsection 3.2.4.

3.2.4 DotHandler.py

The `DotHandler` class has been created in order to manage separately and better the post-processing of the DFA, in *.dot* format, resulting from the computation of MONA. Indeed, since MONA has been developed for different purposes, its output has an additional initial state and transition that to our intent are completely meaningless.

Additionally, the interaction with the *.dot* format has been implemented thanks to the `dotpy` library (available on GitHub⁴) developed for this specific purpose paying particular attention to performances.

As we can see in the implementation of the `DotHandler` class in Listing 3.7, the main methods are `modify_dot` and `output_dot`.

Listing 3.7. The `DotHandler` class.

```

1 from dotpy.parser.parser import MyParser
2 import os
3
4 class DotHandler:
5
6     def __init__(self, path='./inter-automa.dot'):
7         self.dot_path = path
8         self.new_digraph = None
9
10    def modify_dot(self):
11        if os.path.isfile(self.dot_path):
12            parser = MyParser()
13            with open(self.dot_path, 'r') as f:
14                dot = f.read()
15                f.close()
16
17            graph = parser(dot)
18            if not graph.is_singleton():
19                graph.delete_node('0')
20                graph.delete_edge('init', '0')
21                graph.delete_edge('0', '1')
22                graph.add_edge('init', '1')
23            self.new_digraph = graph
24        else:
25            print('[ERROR] No file DOT exists')
26            exit()
27
28    def delete_intermediate_automaton(self):
29        if os.path.isfile(self.dot_path):
30            os.remove(self.dot_path)

```

⁴<https://github.com/Francesco17/dotpy>

```

31         return True
32     else:
33         return False
34
35     def output_dot(self, result_path='./automa.dot'):
36         try:
37             if self.delete_intermediate_automaton():
38                 with open(result_path, 'w+') as f:
39                     f.write(str(self.new_digraph))
40                     f.close()
41             else:
42                 raise IOError('[ERROR] Something wrong occurred in \
43                     the elimination of intermediate automaton.')
44         except IOError:
45             print('[ERROR] Problem with the opening of the file %s!' \
46                 %result_path)

```

The former method at line 10 takes advantage of the APIs exposed by `dotpy`. Especially, it parses the `.dot` file output of MONA (Figure 3.2a), deletes the starting node 0 and the edge from node 0 to node 1 and, finally, makes node 1 initial. Consequently, the latter method at line 35 manages the output of the final post-processed DFA (Figure 3.2b) and stores it in the main directory. For instance, in Figure 3.2 we can see graphically what is the outcome of the post-processing of the automaton corresponding to the formula $\varphi = \Box(a \rightarrow \Box b)$.

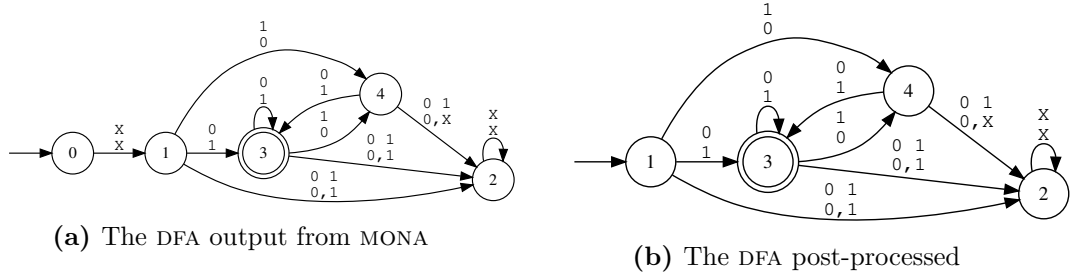


Figure 3.2. Before and after DFA post-processing

3.3 Comparison with FLLOAT

In this section, we will see how LTL_f2DFA performs compared to `FLLOAT`⁵, which is another Python package having the conversion of an LTL_f formula to a DFA as one of its features. In particular, `FLLOAT` handles LTL_f and LDL_f (*Linear Dynamic Logic on Finite Traces*) formulas, but not $PLTL$ ones, but it provides support for syntax,

⁵<https://github.com/MarcoFavorito/flloat>

semantics and parsing of PL (*Propositional Logic*), LTL_f and LDL_f formal languages. Additionally, its conversion is based on a different theoretical result with respect to LTL_f2DFA . Nevertheless, we can compare them on the generation of a DFA from an LTL_f formula.

The time execution benchmarks between these two packages was done over a set of 13 different interesting LTL_f formulas of different length. The comparison consisted of executing each package over the same set of formulas n number of times and, then, repeating the multiple execution m number of times. Thus, for each formula to be converted we obtained $n \times m$ results and, finally, we kept the minimum one (i.e. the best time execution result). After gathering the results, we can show them on a histogram where on the x -axis there are the LTL_f formulas and on the y -axis there is the minimum time (in seconds) needed for the package to convert it into a DFA (Figure 3.3). In the

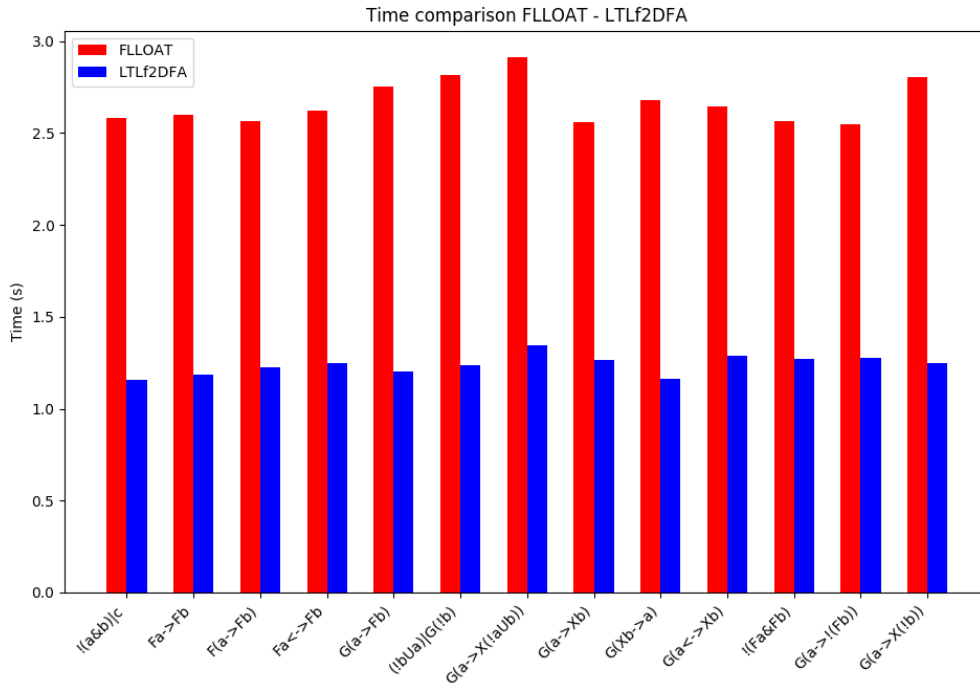


Figure 3.3. Time benchmarking of LTL_f2DFA wrt FLLOAT.

histogram, FLLOAT results are coloured in red, while LTL_f2DFA ones are depicted in blue. As we can see from the bar chart, in both packages the time needed to convert the formula increases as the length of the formula grows. However, it is notable that LTL_f2DFA is overall twice as fast as FLLOAT. This behaviour is due to the fact that these two packages operate in a different way. Indeed, while FLLOAT is a pure Python package, LTL_f2DFA uses, for the heavy task of the generation of the automaton, MONA that is written in C++. Hence, the real difference relies on the performance differences between C++ and Python programs. As a final remark, although LTL_f2DFA is much

faster than FLLOAT, its time execution depends on the I/O system performance which can drastically reduce it. Thus, LTL_f2DFA results may arise depending on various factors such as disk speed, caching and filesystem.

3.4 Discussion

In this chapter, we have presented the LTL_f2DFA Python package. We have also described the structure of the package, discussed in detail its implementation highlighting all the main features and, finally, seen how it performs in time relatively to the FLLOAT Python package.

Chapter 4

Janus

In this chapter, we will illustrate how our tool LTL_f2DFA presented in Chapter 3 can be efficiently employed in the field of Business Process Modeling, with particular attention to Process Mining. First of all, we will formally describe the theoretical framework of declarative process mining. Then, in this context, we will thoroughly describe the implementation of the Janus algorithm (Cecconi et al., 2018) for computing the interestingness degree of traces.

Chapter 5

DFAgame

Chapter 6

Conclusions and Future Work

Continue the introduction and possible future work

Bibliography

- Morten Biehl, Nils Klarlund, and Theis Rauhe. Algorithms for guided tree automata. In *International Workshop on Implementing Automata*, pages 6–25. Springer, 1996.
- Alessio Cecconi, Claudio Di Ciccio, Giuseppe De Giacomo, and Jan Mendling. Interestingness of traces in declarative process mining: The janus ltlpf approach. In *International Conference on Business Process Management*, pages 121–138. Springer, 2018.
- Giuseppe De Giacomo and Moshe Y. Vardi. Linear temporal logic and linear dynamic logic on finite traces. In *IJCAI*, volume 13, pages 854–860, 2013.
- Giuseppe De Giacomo and Moshe Y. Vardi. Synthesis for ltl and ldl on finite traces. In *Proceedings of the 24th International Conference on Artificial Intelligence*, IJCAI’15, pages 1558–1564. AAAI Press, 2015. ISBN 978-1-57735-738-4. URL <http://dl.acm.org/citation.cfm?id=2832415.2832466>.
- Giuseppe De Giacomo, Riccardo De Masellis, and Marco Montali. Reasoning on ltl on finite traces: Insensitivity to infiniteness. In *Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence*, AAAI’14, pages 1027–1033. AAAI Press, 2014. URL <http://dl.acm.org/citation.cfm?id=2893873.2894033>.
- Jacob Elgaard, Nils Klarlund, and Anders Møller. MONA 1.x: new techniques for WS1S and WS2S. In *Proc. 10th International Conference on Computer-Aided Verification (CAV)*, volume 1427 of *LNCS*, pages 516–520. Springer-Verlag, June/July 1998.
- D. Gabbay, A. Pnueli, S. Shelah, and J. Stavi. On the temporal analysis of fairness. Technical report, Jerusalem, Israel, Israel, 1997.
- Dov Gabbay, Amir Pnueli, Saharon Shelah, and Jonathan Stavi. On the temporal analysis of fairness. In *Proceedings of the 7th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 163–173. ACM, 1980.
- Valentin Goranko and Antony Galton. Temporal logic. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, winter 2015 edition, 2015.

- Jesper G Henriksen, Jakob Jensen, Michael Jørgensen, Nils Klarlund, Robert Paige, Theis Rauhe, and Anders Sandholm. *Mona: Monadic second-order logic in practice*. In *International Workshop on Tools and Algorithms for the Construction and Analysis of Systems*, pages 89–110. Springer, 1995.
- Hans Kamp. *Tense Logic and the Theory of Linear Order*. PhD thesis, University of California Los Angeles, 1968. URL <http://www.ims.uni-stuttgart.de/archiv/kamp/files/1968.kamp.thesis.pdf>. Published as Johan Anthony Willem Kamp.
- Nils Klarlund and Anders Møller. *MONA Version 1.4 User Manual*. BRICS, Department of Computer Science, Aarhus University, January 2001. Notes Series NS-01-1. Available from <http://www.brics.dk/mona/>. Revision of BRICS NS-98-3.
- Nicolas Markey. Temporal logic with past is exponentially more succinct. *EATCS Bulletin*, 79:122–128, 2003.
- Amir Pnueli. The temporal logic of programs. In *Proceedings of the 18th Annual Symposium on Foundations of Computer Science*, SFCS '77, pages 46–57, Washington, DC, USA, 1977. IEEE Computer Society. doi: 10.1109/SFCS.1977.32. URL <https://doi.org/10.1109/SFCS.1977.32>.
- M. O. Rabin and D. Scott. Finite automata and their decision problems. *IBM J. Res. Dev.*, 3(2):114–125, April 1959. ISSN 0018-8646. doi: 10.1147/rd.32.0114. URL <http://dx.doi.org/10.1147/rd.32.0114>.
- A. P. Sistla and E. M. Clarke. The complexity of propositional linear temporal logics. *J. ACM*, 32(3):733–749, July 1985. ISSN 0004-5411. doi: 10.1145/3828.3837. URL <http://doi.acm.org/10.1145/3828.3837>.
- Shufang Zhu, Pu Geguang, and Moshe Y. Vardi. First-order vs. second-order for ltlf-to-automata: An extended abstract. *Women in Logic*, 2018.