Time Modalities over Many-valued Logics

Nicholas Fiorentini[1], Achille Frigeri[1], Liliana Pasquale[2], and Paola Spoletini[3]

[1] Politecnico di Milano
fiorentini@studenti.polimi.it,achille.frigeri@polimi.it
[2] University of Limerick liliana.pasquale@lero.ie
[3] Università dell'Insubria paola.spoletini@uninsubria.it

1 Introduction

Model checking has been traditionally concerned on verifying a (critical) system against its specification, which is generally expressed in temporal logic. Despite this verification technique is mature, it becomes useless when the specification incorporates vagueness, especially for the temporal constraints. This is often the case when non-critical adaptive systems are considered. These systems may tolerate small violations or may need to be aware of the satisfaction degree of their specification for re-configuration purposes. We present FTL (Fuzzy-time Temporal Logic), an extension of LTL that relaxes the notion of time, and propose a verification technique to evaluate the truth degree of such vague temporal properties. Our verification technique has been implemented in a prototype and the experimental results are promising.

2 FTL: Fuzzy-Time Temporal Logic

FTL (Fuzzy-Time Temporal Logic) [1] is a language conceived to express specifications for system hampered by uncertainty and vagueness, extending LTL by adding a set of temporal operators to express vague temporal properties.

Syntax Let F be a numerable set of atomic (crisp or fuzzy) propositions, $\neg$, $\wedge$, $\vee$, $\Rightarrow$ be the (fuzzy) logical connectives, and O and T the sets of unary and binary (fuzzy) temporal modalities. Then, φ belongs to the set Φ of *well-formed FTL formulae* (from now on, formulae), if it is defined as follows: $\varphi := p \mid \neg\varphi \mid \varphi \sim \varphi \mid \mathcal{O}\varphi \mid \varphi \mathcal{T} \varphi$, where $p \in F$, $\sim$ is a binary connective, $\mathcal{O} \in O$, and $\mathcal{T} \in T$. As unary operators we consider $\mathcal{X}$ (next), $\mathcal{S}oon$ (soon), $\mathcal{F}$ (eventually), $\mathcal{F}_t$ (eventually in the next t instants), $\mathcal{G}$ (always), $\mathcal{G}_t$ (always in the next t instants), $\mathcal{AG}$ (almost always), $\mathcal{AG}_t$ (almost always in the next t instants), $\mathcal{L}_t$ (lasts t instants), $\mathcal{W}_t$ (within t instants), where $t \in \mathbb{N}$; binary operators are $\mathcal{U}/\mathcal{U}_t$ (until/until with t instants), $\mathcal{AU}/\mathcal{AU}_t$ (almost until/almost until within t instants).

Semantics The semantics of a formula φ is defined w.r.t. a linear structure (S, s_0, π, L), where S is the set of states, s_0 is the initial state, π is an infinite path $\pi = s_0 s_1 \cdots \in S^\omega$, π^i is the suffix of π starting from the i-th position and

s^i is its first state. $L : S \to [0,1]^F$ is the *(fuzzy) labeling function* that assigns to each atomic proposition in F its corresponding evaluation at each state. Besides, we adopt an *avoiding function*, $\eta : \mathbb{Z} \to [0,1]$. We assume $\eta(i) = 1$ for all $i \leq 0$, η is strictly decreasing in $\{0, \ldots, n_\eta\}$ for some $n_\eta \in \mathbb{N}$, and $\eta(n') = 0$ for all $n' \geq n_\eta$. Since we are dealing with a multi-valued logic, we define the semantics of a formula via a *fuzzy satisfiability relation* $\models \subseteq S^\omega \times F \times [0,1]$, where $(\pi \models \varphi) = \nu \in [0,1]$ means that the truth degree of φ on π is ν. FTL is defined as a family of logics, where the semantics of connectives is given on a generic t-norm based logic [2]. We use the Gödel-Dummet interpretation for connectives, since this is t-norm based logic that can include the same interpretation of $\wedge$ and $\vee$ as in Zadeh logic. In particular, for an untimed sub-formula we have:

$$(\pi^i \models p) = L(s^i)(p), \qquad (\pi^i \models \varphi \wedge \psi) = \min\{(\pi^i \models \varphi), (\pi^i \models \psi)\}$$

$$(\pi^i \models \neg\varphi) = \begin{cases} 1, (\pi^i \models \varphi) = 0 \\ 0, (\pi^i \models \varphi) > 0 \end{cases} \qquad (\pi^i \models \varphi \vee \psi) = \max\{(\pi^i \models \varphi), (\pi^i \models \psi)\}$$

$$(\pi^i \models \varphi \Rightarrow \psi) = \begin{cases} 1, (\pi^i \models \varphi) \leq (\pi^i \models \psi) \\ 0, (\pi^i \models \varphi) > (\pi^i \models \psi) \end{cases}$$

where $p \in F$, $i \in \mathbb{N}$. The semantics of temporal operators, except for $\mathcal{AG}_t$, $\mathcal{AG}$, $\mathcal{AU}_t$, and $\mathcal{AU}$, is summarized in Figure 1.

Φ	$\pi^i \models \Phi$	Φ	$\pi^i \models \Phi$
$\mathcal{X}\varphi$	$\pi^{i+1} \models \varphi$	$\mathcal{S}oon\,\varphi$	$\max_{i<j\leq i+n_\eta} (\pi^j \models \varphi) \cdot \eta(j-i-1)$
$\mathcal{F}_t\varphi$	$\max_{i\leq j\leq i+t} (\pi^j \models \varphi)$	$\mathcal{W}_t\varphi$	$\max_{i\leq j<i+t+n_\eta} (\pi^j \models \varphi) \cdot \eta(j-t-i)$
$\mathcal{F}\varphi$	$\lim_{t\to+\infty} (\pi^i \models \mathcal{F}_t\varphi)$	$\mathcal{L}_t\varphi$	$\max_{0\leq j\leq \min\{n_\eta,t\}} (\pi^i \models \mathcal{G}_{t-j}\varphi) \cdot \eta(j)$
$\mathcal{G}_t\varphi$	$\min_{i\leq j\leq i+t} (\pi^j \models \varphi)$	$\varphi\,\mathcal{U}_t\,\psi$	$\max_{i\leq j\leq i+t} \{\min\{\pi^j \models \psi, \pi^i \models \mathcal{G}_{j-1}\varphi\}\}$
$\mathcal{G}\varphi$	$\lim_{t\to+\infty} (\pi^i \models \mathcal{G}_t\varphi)$	$\varphi\,\mathcal{U}\,\psi$	$\lim_{t\to+\infty} (\pi^i \models \varphi\,\mathcal{U}_t\,\psi)$

Fig. 1. Semantics for FTL temporal operators.

Informally, $\mathcal{X}$, $\mathcal{G}$ and $\mathcal{F}$ are interpreted as classical LTL operators, except in that the classical connectives used in their sub-formula are associated with their fuzzy interpretation. $\mathcal{G}_t$ and $\mathcal{F}_t$ are the bounded version of $\mathcal{G}$ and $\mathcal{F}$, respectively. $\mathcal{S}oon$ extends $\mathcal{X}$ by tolerating at most n_η time units delay. $\mathcal{W}_t$ means a property is supposed to hold in at least one of the next t time units or, possibly, in the next $t + n_\eta$ time units. An increasing penalization is applied in case a property holds after the t-th time unit. $\mathcal{L}_t$ expresses that a property should last for t consecutive time units. In case a property does not hold from a certain time unit $n \in [0,t]$, a penalization is given depending on the difference between n and t. $\mathcal{AG}$ evaluates a property by avoiding at most n_η worse cases (i.e., where a property is minimally satisfied). A penalization will be assigned according to the number of avoided worse cases (k). If more worse cases are avoided, penalization will be more severe. Hence, a tradeoff should be identified between the number of avoided worse cases and the assigned penalization. Formally, if $\mathcal{P}^k(\mathbb{N})$ is the

set of subsets of $\mathbb{N}$ of cardinality k, then

$$(\pi^i \models \mathcal{AG}\,\varphi) = \max_{k\in\mathbb{N}} \max_{H\in\mathcal{P}^k(\mathbb{N})} \min_{\substack{j\geq i,\\ j\neq i+h,\\ h\in H}} (\pi^j \models \varphi \cdot \eta(k)).$$

$\mathcal{AG}_t$ is the bounded version of $\mathcal{AG}$, in which the index k is supposed to be in $\{0,\ldots,\min n_\eta, t\}$. The semantics $\mathcal{AU}$ and $\mathcal{AU}_t$, is defined similarly to $\mathcal{U}$ and $\mathcal{U}_t$, by replacing the occurrence of $\mathcal{G}_{j-1}$ by $\mathcal{AG}_{j-1}$ (see Figure 1). Under the assumption that all events are crisp, FTL reduces to LTL, formally:

Theorem 1. *Let for all $p \in AP$ and $i \in \mathbb{N}$, $\pi^i \models p \in \{0,1\}$, and $\eta(1) = 0$. Then FTL reduces to LTL.*

We also provide an adequate set, i.e., a subset of its connectives and temporal operators that is sufficient to equivalently express any formula of the logic. Before, we need to introduce the extra operators $\odot^j$, for $1 \leq j < n_\eta$, whose semantics is defined by $(\pi^i \models \odot^j\varphi) = (\pi^i \models \varphi) \cdot \eta(j)$.

Theorem 2. *A set of adequate connectives is $\{\wedge, \Rightarrow, \mathcal{X}, \mathcal{U}, \mathcal{AU}, \odot^1, \ldots, \odot^{n_\eta-1}\}$.*

3 Evaluating formulae

Describing systems with vague conditions FTL formulae are used to express properties of a system described via a Fuzzy discrete Timed Automata (FTA) [3]. FTA are an enriched version of timed automata (TA), introduced by Alur and Dill [4] to describe real-time systems. Analogously to TA, FTA have the capability of manipulating clocks, which evolve continuously and synchronously with absolute time. FTA extend classical finite automata to fuzzy events, which in many contexts are more suitable to describe realistic systems. The domain of our FTA is $\mathbb{N}$, since this is the same domain chosen for FTL. FTA are defined over a finite set of clocks, a finite set of crisp events, and a finite set of control variables. The range over which these variables vary represents the support for fuzzy events. The clock values change while the automaton stays in a location and can be reset when a transition is taken. Instead, control variables may change their value, within the limit of their range, both in a location or when a transition is taken. Each transition of this automaton is labeled with constraints on both clock values and fuzzy attributes, which may also be related to the value of control variables. Then, an FTA is a finite state automaton on infinite words in which locations are connected through Event-Condition-Action (ECA) rules. The condition of a ECA rule is the conjunction of a temporal and a fuzzy constraint (a fuzzy event is implicitly a fuzzy condition on the values of the attributes on a support). Starting from the source location, a transition is performed if the specified events occur and the conditions are satisfied. Once it is performed, the corresponding actions (i.e., reset of a subset of the variables in $T \cup F$ and the increasing or decreasing of a subset of the control variables in F) are performed as well, and the target location is reached. The values of control

variables can also be changed in the location, defining the variation period. Analogously to TA, the semantics of FTA is described through a Timed Transition System (TTS), in which states represent a snapshot of the automaton during its evolution. Each state includes the current location, the value of the clocks in T, the set of events that just occurred, and the value of the control variables. The transitions between states can be of three types: discrete, purely timed or support timed. Discrete transitions represent the transition of the automaton, purely timed transitions describe the time passed within a location and support timed transitions represent the support variations within a location.

Evaluation algorithm An FTL formula is evaluated on a FTA not as true or false, but by associating to it a truth degree in $[0, 1]$.
The evaluation algorithm is composed of the following three phases:

1. Preprocessing of the FTL formula: the property is rewritten in terms of min and max and the parsing tree of the translated formula is annotated with the corresponding intervals under consideration;
2. Building a finite version of the TTS (FTTS) using temporal zones, as in [5];
3. Formula evaluation: the truth degree of the formula is computed on FTTS.

Step 1 is independent from step 2, but it needs to be performed before step 3. Steps 2–3 can be seen as the stages of a pipeline, since they can be executed in parallel and mutually synchronize on the inter-stage results.

4 Conclusions

We proposed an innovative approach for evaluating vague temporal formulae. Our technique computes the minimum and the maximum truth degree a given formula can have in an automata-based model (FTA) of the system. Each formula is expressed according to FTL, a fuzzy time temporal logic, and can assume any value in the interval $[0, 1]$. We provided a prototype that implements the evaluation technique, and performed a set of experiments on a simple case study. The preliminary results are encouraging and demonstrate the feasibility of the approach. As a future work we aim to further improve the performance of the checking technique and study its complexity bounds.

References

1. Frigeri, A., Pasquale, L., Spoletini, P.: Fuzzy Time in LTL. CoRR abs/1203.6278
2. Hájek, P.: Metamathematics of Fuzzy Logic. Kluwer (1998)
3. Fiorentini, N., Pasquale, L., Spoletini, P.: Evaluating vague temporal properties. In: Submitted to Formats 2012. (2012)
4. Alur, R., Dill, D.L.: A Theory of Timed Automata. TCS **126** (1994) 183–235
5. Bengtsson, J., Yi, W.: Timed automata: Semantics, algorithms and tools. In: Lectures on Concurrency and Petri Nets. (2003) 87–124