Combining the Temporal and Epistemic Dimensions for MTL Monitoring

Eugene Asarin[1], Oded Maler[2], Dejan Nickovic[3], and **Dogan Ulus**[2],

[1] Irif, Université Paris Diderot, France
[2] Verimag, CNRS & Université Grenoble-Alpes (UGA), France
[3] Austrian Institute of Technology (AIT), Austria

September 6, 2017

FORMATS 2017

Outline

- Introduction & Motivation
- Defining 2D MTL
- Monitoring 2D MTL
- Example

Temporal Logic and Infinite Behaviors in Verification

- Temporal logic is typically interpreted over infinite behaviors in one direction. (Time domain is $\mathbb{N}$ or $\mathbb{R}_+$)
- It is assumed that a *model* of the system which provides an effective representation of all those infinite behaviors.
- An ω-automaton is built accepting exactly the infinite sequences that satisfy the specifications.
- Verification (model checking) reduces to testing inclusion between two ω-regular languages. (Vardi & Wolper 86)
- Which can be solved, modulo complexity, by reasoning about cycles in finite-state automata.

Moving to Finite Behaviors: Motivation I

- In many (if not most) real-life situations, exhaustive verification is impossible.
- Instead, simulation-based (runtime, dynamic, lightweight) verification is practiced.
- Behaviors are generated *individually* from a system model, which could be a black box, a dirty software, a simulator.
- Each of these behaviors is checked for property satisfaction: the language inclusion test of verification is replaced by numerous membership tests.
- By definition, such behaviors are finite.
- We use the term *monitoring* for this activity.

Moving to Finite Behaviors: Motivation II

- Monitoring can also be applied to *real systems during their execution*.
- In contrast with verification which is done at the design and development stage.
- We want to detect patterns occurring in behaviors.
- Not necessarily starting at the beginning or continuing until the “end".
- We need an approach where *finite segments of behaviors* are considered as first-class citizens.

The Critical Part

- We want to use MTL formulas in pattern-action sentences:

  Do some action if the formula φ holds.

  in real-time systems during their execution.

- But the formula is satisfied at the end of behavior.
- Problem: The end of behavior moves!!
- We need a 2D semantics for MTL where the second parameter indicates the end of temporal knowledge.
- And we are porting back our 2D experience with TRE to MTL.

Definitions

Common Definitions

- A set P of propositional variables.
- A Boolean signal $w : [0, \ell) \to \mathbb{B}^{|P|}$ over P is a continuous-time function that satisfies the finite-variability condition.
  - Thus w can be partitioned into finitely many intervals.
- The usual syntax of (future) metric temporal logic (MTL):

$$\varphi := p \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \mathcal{U}_I \varphi_2$$

- An equivalent (and easier to work) syntax:

$$\varphi := p \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid F_{[a,b]} \mid \varphi_1 \mathcal{U} \varphi_2$$

as timed until $\varphi_1 \mathcal{U}_{[a,b]} \varphi_2 = G_{[0,a]} \varphi_1 \mathcal{U} \varphi_2 \wedge F_{[a,b]} \varphi_2$.

(We also avoid open-close intervals for the clarity.)

Satisfaction in 2D (Intuitively)

- The usual temporal parameter t.
- The end of the signal as an additional parameter t'.
- We do not know later than t' so our reasoning is limited.
- A formula φ holds at t with respect to t'.
- Hence, the truth value depends on the pair (t, t').

This is similar to pattern matching but the meaning differs.

Satisfaction in 2D (Formally)

Definition (MTL Matching Semantics with Satisfaction Maps)

The matching semantics of MTL formulas with respect to a Boolean signal w is defined inductively as follows:

$$
\begin{aligned}
&p(t,t') = w_p(t) \wedge t < t' < \ell \\
&(\neg\varphi)(t,t') = \neg(\varphi(t,t')) \\
&(\varphi \vee \psi)(t,t') = \varphi(t,t') \vee \psi(t,t') \\
&(F_{[a,b]}\varphi)(t,t') = \bigvee_{r \in [t+a,t+b]} \varphi(r,t') \\
&(\varphi_1 \mathcal{U} \varphi_2)(t,t') = \bigvee_{r \geq t} (\varphi_2(r,t') \wedge \bigwedge_{r' \in [t,r]} \varphi_1(r',t'))
\end{aligned}
$$

Monitoring MTL with 2D semantics

Previously for timed pattern matching

Definition (Match Sets)

A segment (t, t') of the signal w matches a timed regular expression φ, denoted as $(w, t, t') \models \varphi$. The match-set of φ in w is the set of all matching segments:

$$\mathcal{M}(\varphi, w) = \{(t, t') : (w, t, t') \models \varphi\}.$$

- We showed match sets can be representable by finite unions of 2D zones and provided algorithms for regular operations including intersection on zones.

For MTL, I'll use the term **valuation** for the set of all pairs (t, t') satisfying the formula φ, denoted $V(\varphi, w)$. It also turns out to be representable by finite unions of 2D zones.

Representations in 2D

Definition (Zones)

A two-dimensional zone Z is a subset of $\mathbb{R}^2_+$ which is defined via a conjunction of orthogonal and difference inequalities of the following form

$$\begin{array}{c} \underline{\alpha} \prec t \prec \overline{\alpha} \\ \underline{\beta} \prec t' \prec \overline{\beta} \\ \underline{\gamma} \prec t' - t \prec \overline{\gamma} \end{array} \tag{1}$$

Definition (Timed Polyhedron)

A timed polyhedron $\mathbf{Z}$ is a subset of $\mathbb{R}^2_+$ expressible as a Boolean combination of orthogonal and difference constraints as in (1). A set of zones $\mathcal{Z} = \{Z_1, \ldots, Z_k\}$ is a representation of $\mathbf{Z}$ if

$$\mathbf{Z} = \bigcup_i Z_i$$

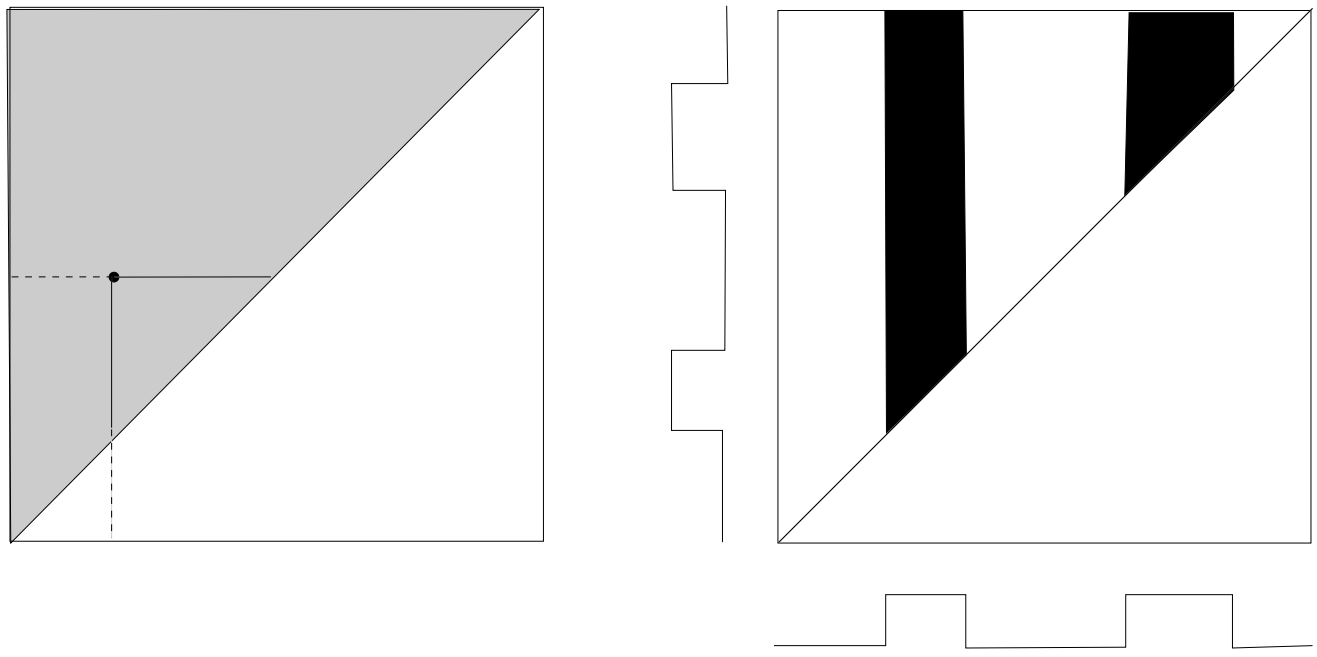
What we need more

- We can represent valuations of atomic propositions as finite union of zones.
- Recall the MTL syntax:

$$\varphi := p \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid F_{[a,b]}\ \varphi \mid \varphi_1 \mathcal{U} \varphi_2$$

- We already have intersection.
- But we still need operations on union of zones for
  - Complementation,
  - Timed Eventuality, and
  - Untimed Until.

Atomic Propositions

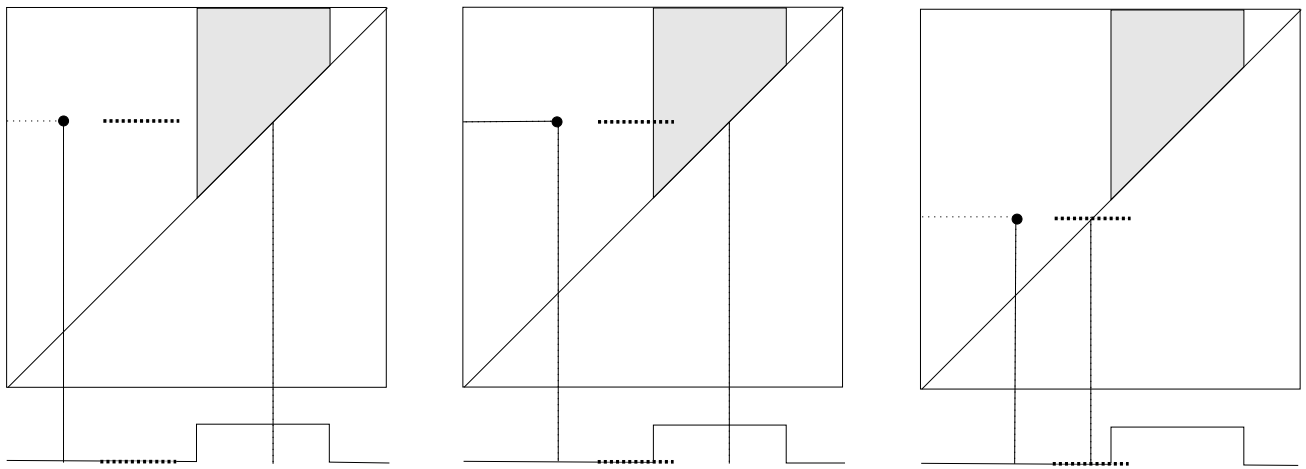


- (Left) The set of all non-empty segments of w can be represented by the triangle $T_w = \{(t, t') : 0 \leq t < t' \leq \ell\}$.
- (Right) Valuations of an atomic proposition for the signal given.

Complementation

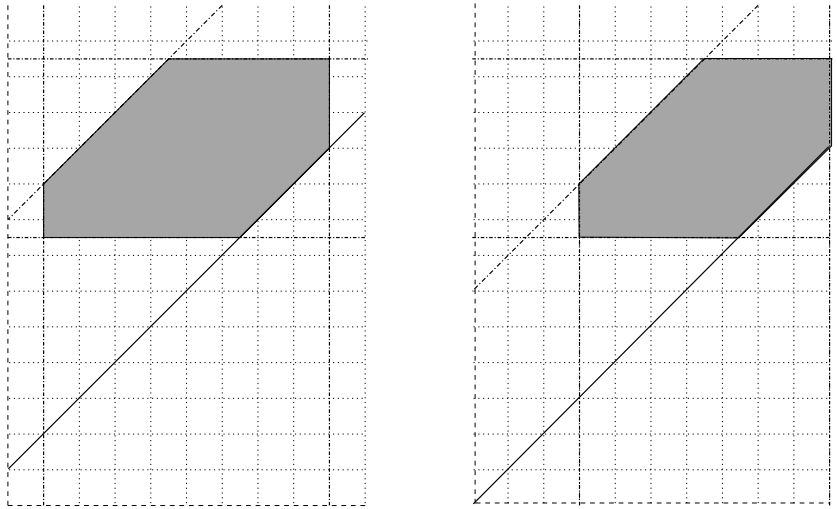
- Timed polyhedra are closed under complementation.
- The complement of a zone is a union of at most six zones (DeMorgan-1).
- The complement of a union of zones is an intersection of complemented zones (DeMorgan-2).
- An expensive computational problem, which we exploit inherent ordering of zones when intersecting out.

Timed Eventuality – Back Shifting



- $\varphi = F_{[a,b]}\ p$
- (Left) The segment does not satisfy φ. (Usual)
- (Middle) The segment satisfy φ. (Usual)
- (Right) The segment does not satisfy φ. (The signal ends.)

Timed Eventuality – Back Shifting



- $Z_{LEFT} = F_{[a,b]}\ Z_{RIGHT}$
- Intuitively, the left vertices are shifted by b and the right by a.
- Precisely,

$$\underline{\alpha} - b \leq t \leq \overline{\alpha} - a$$
$$\underline{\beta} \leq t' \leq \overline{\beta}$$
$$\underline{\gamma} + a \leq t' - t \leq \overline{\gamma} + b$$

- Extended straightforwardly for unions of zones.

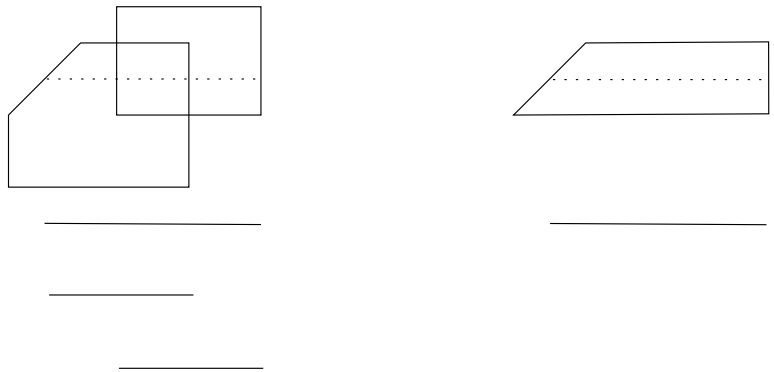
Untimed Until – Single Zones

- We showed in the paper the until operation between two zones yields a zone.

$$Z_1 \,\mathcal{U}\, Z_2 = \left\{ \begin{array}{ccccc} \underline{\alpha}_1 & \prec & t & \prec & \min\{\overline{\alpha}_1, \overline{\alpha}_2\} \\ \max\left\{ \begin{array}{c} \underline{\beta}_1, \underline{\beta}_2, \\ \underline{\alpha}_2 + \underline{\gamma}_1 \end{array} \right\} & \prec & t' & \prec & \min\left\{ \begin{array}{c} \overline{\beta}_1, \overline{\beta}_2, \\ \overline{\alpha}_1 + \overline{\gamma}_2 \end{array} \right\} \\ \max\{\underline{\gamma}_1, \underline{\gamma}_2\} & \prec & t' - t & \prec & \overline{\gamma}_1 \end{array} \right\}$$

- It does not straightforwardly extends to unions of zones.
- In general, applying the until pairwise between sets of zones yields a subset of the correct valuation.

Untimed Until – Single Zones



- For example, consider two zones at left.
- Neither zone contains a maximal interval (dotted line).
- Pairwise until operation between zones cannot cover this case.
- However, guaranteeing all "maximal" zones in the representation would prevent this problem. (Such as the zone at right)

The Beautiful Theory of Boolean Functions

- Canonical expressions in Boolean Algebra, Archie Blake (1937)
  - The disjunction of all prime implicants is a canonical form.
  - Computed by double negation. (with many discoverer)
- We can directly apply his theory using these correspondences:

Boolean function	—	Timed polyhedron
DNF	—	Union of zones
Implicant	—	Zone
Prime implicant	—	Maximal Zone

- Then we define the maximal normal form of timed polyhedra.

Definition (Maximal Zones, Maximal Normal Form)

Let $\mathbf{Z}$ be a timed polyhedron. A zone $Z \subseteq \mathbf{Z}$ is maximal in $\mathbf{Z}$ if there is no other zone Z' such that $Z \subset Z' \subseteq \mathbf{Z}$. A representation $\mathcal{Z}$ of $\mathbf{Z}$ is maximal if contains all maximal zones. A representation is reduced maximal if it consists of the set of all maximal zones.

Untimed Until – Unions of Zones

- Pairwise Operation on Maximal Representations:
  Let $V(\varphi_1) = \mathbf{Z}_1$ and $V(\varphi_2) = \mathbf{Z}_2$ be timed polyhedra, represented by $\mathcal{Z}_1$ and $\mathcal{Z}_2$, respectively, with $\mathcal{Z}_1$ being maximal. Then $V(\varphi_1 \mathcal{U} \varphi_2)$ is also a timed polyhedron computed as

$$\bigcup_{Z_1 \in \mathcal{Z}_1} \bigcup_{Z_2 \in \mathcal{Z}_2} {}^{\cdot}(Z_1, Z_2).$$

And finally we have,

Theorem (Valuations for 2D MTL)

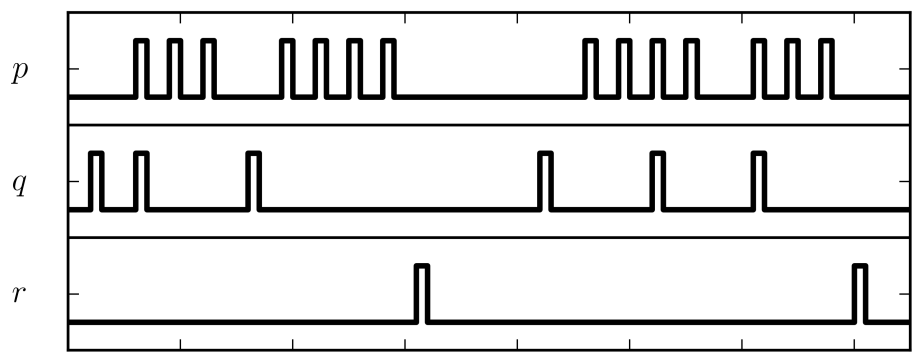
For any MTL formula φ and a finite variability Boolean signal w, $V(\varphi, w)$ is a timed polyhedron represented as a finite union of zones.

Example Property

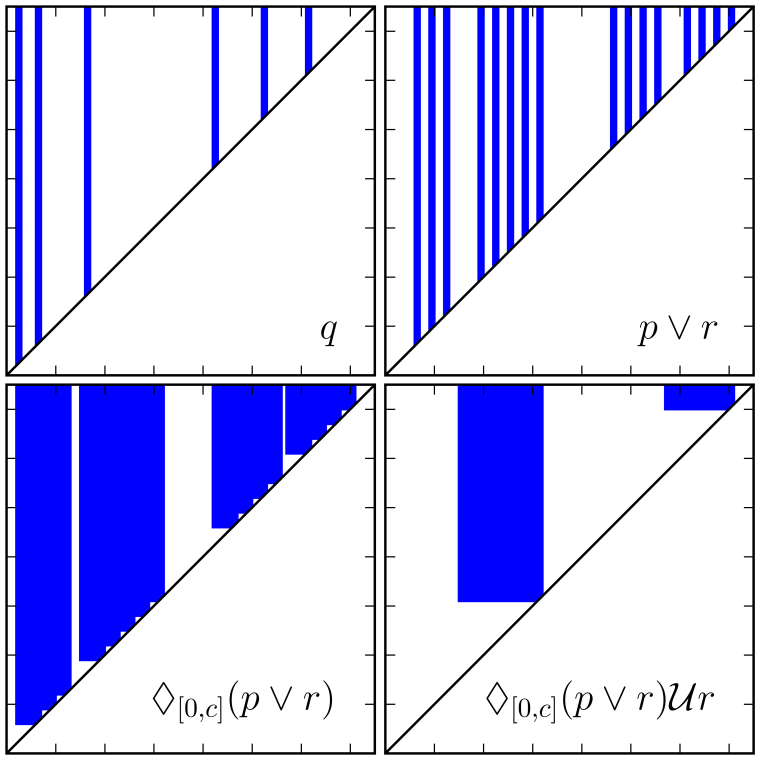
- We consider a bounded recurrence property:

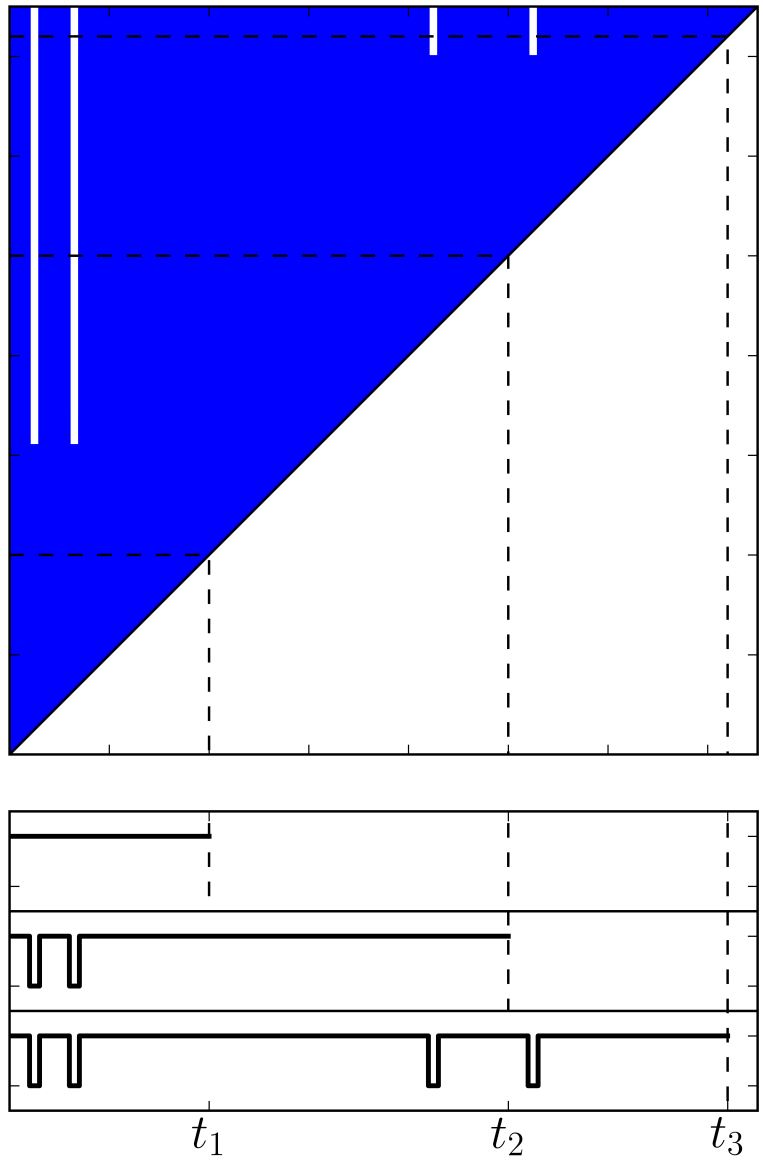
$$\varphi_1 \;:=\; (q \wedge \neg r \wedge Fr) \rightarrow (F_{[0,c]}(p \vee r)\, \mathcal{U}\; r)$$

- Property φ_1 requires proposition p to hold at least every c time units between q and r.
- Such properties are commonly used to express periodic tasks to be performed between two events.
- The input signal is below.



Example Property





Concluding Remarks

- We defined a 2D semantics for MTL by taking the end of signal as a parameter.
- We exported and adapted the two-dimensional matching technology from TREs to MTL.
- On the way, we developed maximal normal forms, complementation, eventuality, and until operations therein.
- These techniques can also handle naturally two dimensional logics such as Halpern-Shoham, CDT logic, and their metric extensions.

Thank you for your attention!