Optimal Enforcement of (Timed) Properties with Uncontrollable Events
Matthieu Renard, Yliès Falcone, Antoine Rollet, Thierry Jéron, Hervé Marchand

To cite this version:

HAL Id: hal-01262444
https://hal.archives-ouvertes.fr/hal-01262444v4
Submitted on 9 May 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Optimal Enforcement of (Timed) Properties with Uncontrollable Events

MATTHIEU RENARD¹, YLIÈS FALCONE², ANTOINE ROLLET¹, THIERRY JÉRON³, and HERVÉ MARCHAND³

¹ LaBRI, Bordeaux INP, Université Bordeaux, Bordeaux, France.
³ Inria Rennes Bretagne-Atlantique, Rennes, France.

Received April 2017

This paper deals with runtime enforcement of untimed and timed properties with uncontrollable events. Runtime enforcement consists in defining and using mechanisms that modify the executions of a running system to ensure their correctness with respect to a desired property. We introduce a framework that takes as input any regular (timed) property described by a deterministic automaton over an alphabet of events, with some of these events being uncontrollable. An uncontrollable event cannot be delayed nor intercepted by an enforcement mechanism. Enforcement mechanisms should satisfy important properties, namely soundness, compliance, and optimality - meaning that enforcement mechanisms should output as soon as possible correct executions that are as close as possible to the input execution. We define the conditions for a property to be enforceable with uncontrollable events. Moreover, we synthesise sound, compliant, and optimal descriptions of runtime enforcement mechanisms at two levels of abstraction to facilitate their design and implementation.

1. Introduction

Runtime verification (Leucker and Schallhart, 2009; Falcone et al., 2013) is a powerful technique which aims at checking the conformance of the executions of a system under scrutiny with respect to some specification. It consists in running a mechanism that assigns verdicts to a sequence of events produced by the instrumented system with respect to a property formalising the specification. This paper focuses on runtime enforcement (cf. (Schneider, 2000; Ligatti et al., 2009; Falcone et al., 2011; Basin et al., 2013)) which goes beyond pure verification at runtime and studies how to react to a violation of specifications. In runtime enforcement, an enforcement mechanism (EM) takes a (possibly incorrect) execution sequence as input, and outputs a new sequence. Enforcement mechanisms should be sound and transparent, meaning that the output should satisfy the property under consideration and should be as close as possible to the input, respectively. When dealing with timed properties, EMs can act as delayers over the input sequence of events (Pinisetty et al., 2012; Pinisetty et al., 2014b; Pinisetty et al., 2014c). That is, whenever possible, EMs buffer input events for some time and then release them in such a way that the output sequence of events satisfies the property. The general scheme is given in Fig. 1.
Motivations. We focus on enforcement of properties with uncontrollable events\(^1\). Introducing uncontrollable events is a step towards more realistic runtime enforcement. Uncontrollable events naturally occur in many application scenarios where the EM has no control over certain input events. For instance, certain events from the environment may be out of the scope of the mechanism at hand. This situation arises for instance in avionic systems where a command of the pilot has consequences on a specific component. In this critical domain, one usually adds control mechanisms in specific points of the architecture in order to verify that nothing wrong happens. Some events may only be observed by these mechanisms in order to decide if a situation is abnormal, but they cannot be acted upon, meaning that they are uncontrollable. For instance, the “spoiler activation”\(^2\) command triggered by the pilot is sent by the panel to a control flight system, and this leads finally to a specific event on the spoilers. Placing an EM directly on the spoilers prevents events leading to an incoherent state by blocking them, according to the pilot commands. The pilot commands are out of the scope of the EM, i.e. observable but uncontrollable. In the timed setting, uncontrollable events may be urgent messages that cannot be delayed by an enforcement mechanism. Similarly, when a data-dependency exists between two events (e.g., between a write event that displays a value obtained from a previous read event), the first read event is somehow uncontrollable as it cannot be delayed by the enforcement mechanism without preventing the write event from occurring in the monitored program.

Challenges. Considering uncontrollable events in the timed setting induces new challenges. Indeed, EMs may now receive events that cannot be buffered and have to be output immediately. Since uncontrollable events influence the satisfaction of the property under scrutiny, the dates of the controllable events stored in memory have to be recomputed upon the reception of each uncontrollable event to guarantee that the property is still satisfied after outputting them. Moreover, it is necessary to prevent the system from reaching a bad state upon reception of any sequence of uncontrollable events. Since uncontrollable events can occur at any time, the EM must take their potential reception into account when computing the sequence to be emitted. Then, the occurrence of such events has to be anticipated, meaning that all possible sequences of uncontrollable events have to be considered by the enforcement mechanism. It turns out that a property may not be enforceable because of certain input sequences. Intuitively, enforceability issues arise because some sequences of uncontrollable events that lead the property to be violated cannot be avoided. Thus, new enforcement strategies are necessary for both untimed and timed properties.

Contributions. We introduce a framework for the enforcement monitoring of regular untimed and timed properties with uncontrollable events. We define EMs at two levels of abstraction. The synthesised EMs are sound, compliant and optimal. When considering uncontrollable events, it turns out that the usual notion of transparency has to be weakened. As we shall see, the initial

\(^1\) This notion of uncontrollable event should not be confused with the notion of uncontrollable transition used in some supervision and game theory.

\(^2\) The spoiler is a device used to reduce the lift of an aircraft.
Optimal Enforcement of (Timed) Properties with Uncontrollable Events

Order between uncontrollable and controllable events can change in output, contrary to what is prescribed by transparency. Thus, we replace transparency with a new notion, namely compliance, prescribing that the order of controllable events is maintained while uncontrollable events are output as soon as they are received. We define a property to be enforceable with uncontrollable events when it is possible to obtain a sound and compliant EM for any input sequence. In the timed setting, the executions are associated with dates from which the property is enforceable.

This paper revisits and extends a first approach in (Renard et al., 2015). Most definitions were modified to ensure optimality of the EMs for any regular property. Some definitions have been rewritten in a more formal, more modular, and clearer way. All the proofs of soundness, compliance, optimality and equivalence between the different descriptions of the enforcement mechanism are provided. This new framework can also be used without uncontrollable events.

Remark 1. There exist similarities between supervisory control theory (Ramadge and Wonham, 1987; Ramadge and Wonham, 1989) and runtime enforcement. For instance, a supervisor is usually implemented as a monitor deciding at runtime if a command should be activated or not. Supervisory control usually needs a model of the system, and consists in building a supervisor from this model by cutting forbidden states and transitions of uncontrollable events leading to them. Usually, an EM only uses a high-level property. In our work, an EM is equipped with a memory providing many more possibilities of actions, such as keeping and releasing events.

Outline. Section 2 introduces preliminaries and notations. Sections 3 and 4 present the enforcement framework with uncontrollable events in the untimed and timed settings, respectively. In each setting, we define enforcement mechanisms at two levels of abstraction. Section 5 discusses related work. Section 6 presents conclusions and perspectives. Proofs are in Appendix A.

2. Preliminaries and Notation

Untimed Notions. An alphabet is a finite, non-empty set of symbols. A word over an alphabet \( \Sigma \) is a sequence over \( \Sigma \). The set of finite words over \( \Sigma \) is denoted \( \Sigma^* \). The length of a finite word \( w \) is noted \( |w| \), and the empty word is noted \( \epsilon \). \( \Sigma^+ \) stands for \( \Sigma^* \setminus \{\epsilon\} \). A language over \( \Sigma \) is any subset \( L \subseteq \Sigma^* \). The concatenation of two words \( w \) and \( w' \) is noted \( w.w' \) (the dot is omitted when clear from the context). A word \( w' \) is a prefix of a word \( w \), noted \( w' \preceq w \) if there exists a word \( w'' \) s.t. \( w = w'.w'' \). The word \( w'' \) is called the residual of \( w \) after reading the prefix \( w' \), noted \( w'' = w.w'^{-1}.w \). Note that \( w'.w'' = w'.w'^{-1}.w = w \). These definitions are extended to languages in the natural way. A language \( L \subseteq \Sigma^* \) is extension-closed if for any words \( w \in L \) and \( w' \in \Sigma^* \), \( w.w' \in L \). Given a word \( w \) and an integer \( i \) s.t. \( 1 \leq i \leq |w| \), we note \( w(i) \) the \( i \)-th element of \( w \). Given a tuple \( e = (e_1, e_2, \ldots, e_n) \) of size \( n \), for an integer \( i \) such that \( 1 \leq i \leq n \), we note \( \Pi_i(e) \) the projection on the \( i \)-th coordinate, i.e. \( \Pi_i(e) = e_i \). The tuple \( (e_1, e_2, \ldots, e_n) \) is sometimes noted \((\epsilon_1, \epsilon_2, \ldots, \epsilon_n)\) in order to help reading. It can be used, for example, if a tuple contains a tuple. Given a word \( w \in \Sigma^* \) and \( \Sigma' \subseteq \Sigma \), we define the restriction of \( w \) to \( \Sigma' \), noted \( w|_{\Sigma'} \), as the word \( w' \in \Sigma'^* \) whose letters are the letters of \( w \) belonging to \( \Sigma' \) in the same order. Formally, \( \epsilon|_{\Sigma'} = \epsilon \) and \( \forall a \in \Sigma', \forall a \in \Sigma, (w.a)|_{\Sigma'} = w|_{\Sigma'} \cdot a \) if \( a \in \Sigma' \), and \( (w.a)|_{\Sigma'} = w|_{\Sigma'} \) otherwise. We also note \( =_{\Sigma'} \) the equality of the restrictions of two words to \( \Sigma' \); if \( \sigma \) and \( \sigma' \) are two words, \( \sigma =_{\Sigma'} \sigma' \) if \( \sigma|_{\Sigma'} = \sigma'|_{\Sigma'} \). We define in the same way \( \preceq_{\Sigma'} \sigma \preceq_{\Sigma'} \sigma' \) if \( \sigma|_{\Sigma'} \preceq_{\Sigma'} \sigma'|_{\Sigma'} \).
Automata. An automaton is a tuple \((Q, q_0, \Sigma, \rightarrow, F)\), where \(Q\) is the set of states, \(q_0 \in Q\) is the initial state, \(\Sigma\) is the alphabet, \(\rightarrow \subseteq Q \times \Sigma \times Q\) is the transition relation and \(F \subseteq Q\) is the set of accepting states. Whenever \((q, a, q') \in \rightarrow\), we note it \(q \xrightarrow{a} q'\). Relation \(\rightarrow\) is extended to words \(\sigma \in \Sigma^\ast\) by noting \(q \xrightarrow{\sigma} q'\) whenever there exists \(q'' \in (\Sigma^\ast \cup \{\varepsilon\})\) s.t. \(q \xrightarrow{\sigma''} q'' \xrightarrow{\varepsilon} q'\). Moreover, for any \(q \in Q\), \(q \xrightarrow{\varepsilon} q\) always holds. An automaton \(A = (Q, q_0, \Sigma, \rightarrow, F)\) is deterministic if \(\forall q \in Q, \forall a \in \Sigma, (q \xrightarrow{a} q' \land q \xrightarrow{a} q'') \Rightarrow q' = q''\). 

A is complete if \(\forall q \in Q, \forall a \in \Sigma, \exists q' \in Q, q \xrightarrow{a} q'\). A word \(w\) is accepted by \(A\) if there exists \(q \in F\) such that \(q_0 \xrightarrow{w} q\). The language (i.e. set of all words) accepted by \(A\) is denoted by \(L(A)\). A property is a language accepted by an automaton. In the sequel, we assume that a property \(\varphi\) is represented by a deterministic and complete automaton \(A_\varphi\). For example, in Fig. 2, \(Q = \{q_0, q_1, q_2, q_3\}\), the initial state is \(q_0\), \(\Sigma = \{\text{Auth}, \text{LockOff}, \text{LockOn}, \text{Write}\}\), and the transition relation \(\rightarrow\) contains for instance \((q_0, \text{Auth}, q_1), (q_1, \text{LockOn}, q_2),\) and \((q_3, \text{LockOn}, q_3)\).

Timed Languages. Let \(\mathbb{R}_{\geq 0}\) be the set of non-negative real numbers, and \(\Sigma\) a finite alphabet of actions. An event is a pair \((t, a) \in \mathbb{R}_{\geq 0} \times \Sigma\). We define \(\text{date}((t, a)) = t\) and \(\text{act}((t, a)) = a\) the projections of events on dates and actions respectively. A timed word over \(\Sigma\) is a word over \(\mathbb{R}_{\geq 0} \times \Sigma\) whose real parts are ascending, i.e. \(\sigma\) is a timed word if \(\sigma \in (\mathbb{R}_{\geq 0} \times \Sigma)^\ast\) and \(\forall i \in [1; |\sigma| - 1], \text{date}(w(i)) \leq \text{date}(w(i + 1))\). \(\text{tw}(\Sigma)\) denotes the set of timed words over \(\Sigma\). For a timed word \(\sigma = (t_1, a_1), (t_2, a_2), \ldots, (t_n, a_n)\) and an integer \(i, 1 \leq i \leq n, t_i\) is the time elapsed before action \(a_i\) occurs. We naturally extend the notions of prefix and residual to timed words.

We note \(\text{time}(\sigma) = \text{date}(\sigma(|\sigma|))\) for \(\sigma \neq \varepsilon\), and \(\text{time}(\varepsilon) = 0\). We define the observation of \(\sigma\) at time \(t\) as the timed word \(\text{obs}(\sigma, t) = \max_{\sigma' \in \{ \sigma' \mid \sigma' \preceq \sigma \land \text{time}(\sigma') \leq t \}}\), corresponding to the word that would be observed at date \(t\) if events were received at the date they are associated with. We also define the remainder of the observation of \(\sigma\) at time \(t\) as \(\text{nobs}(\sigma, t) = (\text{obs}(\sigma(i)))^{-1} \sigma\), which corresponds to the events that are to be received after date \(t\). The untimed projection of \(\sigma\) is \(\Pi_{\Sigma}(\sigma) = a_1, a_2, \ldots, a_n\), the sequence of actions of \(\sigma\) with dates ignored. \(\sigma\) delayed by \(t \in \mathbb{R}_{\geq 0}\) is the word noted \(\sigma + t\) s.t. \(t\) is added to all dates: \(\sigma + t = (t_1 + t, a_1), (t_2 + t, a_2), \ldots, (t_n + t, a_n)\). Similarly, we define \(\sigma - t\) when \(t_1 \geq t\) to be the word \((t_1 - t, a_1), (t_2 - t, a_2), \ldots, (t_n - t, a_n)\).

We also extend the definition of the restriction of \(\sigma\) to \(\Sigma' \subseteq \Sigma\) to timed words, s.t. \(\varepsilon_{|\Sigma'} = \varepsilon\), and for \(\sigma \in \text{tw}(\Sigma)\) and \((t, a)\) s.t. \(\sigma(t, a) \in \text{tw}(\Sigma)\), \(\Pi_{|\Sigma'}(\sigma(t, a)) = (\sigma_{|\Sigma'})(t, a)\) if \(a \in \Sigma'\), and \((\sigma(t, a))_{|\Sigma'} = \sigma_{|\Sigma'}\) otherwise. The notations \(=_{\Sigma'}\) and \(\preceq_{\Sigma'}\) are then naturally extended to timed words. A timed language is any subset of \(\text{tw}(\Sigma)\). The notion of extension-closed languages is naturally extended to timed languages. We also extend the notion of extension-closed languages to sets of elements composed of a timed word and a date: a set \(S \subseteq \text{tw}(\Sigma) \times \mathbb{R}_{\geq 0}\) is time-extension-closed if for any \((\sigma, t) \in S\), for all \(w \in \text{tw}(\Sigma)\) s.t. \(\sigma.w \in \text{tw}(\Sigma)\), for all \(t' \geq t\), \((\sigma.w, t') \in S\). In other words, \(S\) is time-extension-closed if for every \(\sigma \in \text{tw}(\Sigma)\), there exists a date \(t\) from which \(\sigma\) and all its extensions are in \(S\), that is, associated with a date greater or equal to \(t\). Moreover, we define an order on timed words: we say that \(\sigma'\) is a delayed prefix of \(\sigma\), noted \(\sigma' \preceq_d \sigma\), whenever \(\Pi_{\Sigma}(\sigma') \preceq \Pi_{\Sigma}(\sigma)\) and \(\forall i \in [1; |\sigma'| - 1], \text{date}(\sigma(i)) \leq \text{date}(\sigma'(i))\).
Optimal Enforcement of (Timed) Properties with Uncontrollable Events

Note that the order is not the same in the different constraints: $\Pi_\Sigma(\sigma')$ is a prefix of $\Pi_\Sigma(\sigma)$, but dates in $\sigma'$ exceed dates in $\sigma$. As for the equality $=$ and the prefix order $\preceq$, we note $\sigma' \preceq_{\Pi_\Sigma} \sigma$ whenever $\sigma' \preceq_{\Pi_\Sigma} \sigma$. We also define a lexical order $\leq_{\text{lex}}$ on timed words with identical untimed projections, s.t. $\epsilon \leq_{\text{lex}} \epsilon$, and for two words $\sigma$ and $\sigma'$ s.t. $\Pi_\Sigma(\sigma) = \Pi_\Sigma(\sigma')$, and two events $(t, a)$ and $(t', a), (t', a), \sigma' \leq_{\text{lex}} (t, a), \sigma$ if $t' < t \vee (t = t' \wedge \sigma' \leq_{\text{lex}} \sigma)$.

Consider for example the timed word $\sigma = (1, a), (2, b), (3, c), (4, a)$ over the alphabet $\Sigma = \{a, b, c\}$. Then, $\Pi_\Sigma(\sigma) = a.b.a.a, \text{obs}(\sigma, 3) = (1, a), (2, b), (3, c), \text{obs}(\sigma, 3) = (4, a), \text{and if } \Sigma' = \{b, c\}, \sigma_{\Sigma'} = (2, b) . (3, c)$, and for instance $(1, a) . (2, b) . (4, c) \preceq_{\Pi_\Sigma} \sigma$, and $\sigma \leq_{\text{lex}} (1, a), (3, b). (3, c), (3, a)$. Moreover, if $w = (1, a), (2, b)$, then $w^{-1}.\sigma = (3, c), (4, a)$.

Timed Automata. Let $X = \{X_1, X_2, \ldots, X_n\}$ be a finite set of clocks, i.e. variables that increase regularly with time. A clock valuation is a function $\nu$ from $X$ to $\mathbb{R}_{\geq 0}$. The set of clock valuations for the set of clocks $X$ is noted $\mathcal{V}(X)$, i.e., $\mathcal{V}(X) = \{\nu \mid \nu : X \to \mathbb{R}_{\geq 0}\}$. We consider the following operations on valuations: for any valuation $\nu, \nu + \delta$ is the valuation assigning $\nu(X_i) + \delta$ to every clock $X_i \in X$; for any subset $X' \subseteq X, \nu[X' \leftarrow 0]$ is the valuation assigning 0 to each clock in $X'$, and $\nu(X_i)$ to any other clock $X_i$ not in $X'$. $G(X)$ denotes the set of guards consisting of boolean combinations of constraints of the form $\Xi_i \geq_{\Sigma} w$ with $\Xi_i \in X, w \in \mathbb{N}$, and $\Xi_i \in \{<, \leq, =, \geq, >\}$. Given $g \in G(X)$ and a valuation $\nu$, we write $\nu \models g$ when for every constraint $\Xi_i \geq_{\Sigma} w$ in $g, \nu(\Xi_i) \geq_{\Sigma} w$ holds.

**Definition 1** (Timed automaton (Alur and Dill, 1992)). A timed automaton (TA) is a tuple $A = (L, l_0, X, \Sigma, \Delta, G)$, s.t. $L$ is a set of locations, $l_0 \in L$ is the initial location, $X$ is a set of clocks, $\Sigma$ is a finite set of events, $\Delta \subseteq L \times G(X) \times \Sigma \times 2^X \times L$ is the transition relation, and $G \subseteq L$ is a set of accepting locations. A transition $(l, g, a, X', l') \in \Delta$ is a transition from $l$ to $l'$, labelled with event $a$, with guard $g$, and with the clocks in $X'$ to reset.

The semantics of a timed automaton $A$ is a timed transition system $\langle A \rangle = \langle Q, q_0, \Gamma, \rightarrow, F_G \rangle$ where $Q = L \times \mathcal{V}(X)$ is the (infinite) set of states, $q_0 = (l_0, \nu_0)$ is the initial state, with $\nu_0 = \nu[X \leftarrow 0], F_G = G \times \mathcal{V}(X)$ is the set of accepting states, $\Gamma = \mathbb{R}_{\geq 0} \times \Sigma$ is the set of transition labels, each one composed of a delay and an action. The transition relation $\rightarrow \subseteq Q \times \Gamma \times Q$ is a set of transitions of the form $(l, \nu) \xrightarrow{\delta, a} (l', \nu')$ with $\nu' = (\nu + \delta)[Y \leftarrow 0]$ whenever there is a transition $(l, g, a, Y, l') \in \Delta$ s.t. $\nu + \delta \models g$, for $\delta \geq 0$.

A timed automaton $A = (L, l_0, X, \Sigma, \Delta, G)$ is deterministic if for any different transitions $(l, g_1, a, Y_1, l'_1)$ and $(l, g_2, a, Y_2, l'_2)$ in $\Delta$, $g_1 \wedge g_2$ is unsatisfiable, meaning that only one transition can be fired at any time. $A$ is complete if for any $l \in L$ and any $a \in \Sigma$, the disjunction of the guards of all the transitions leaving $l$ and labelled by $a$ is valid (i.e., it holds for any clock valuation). An example of a timed automaton is given in Fig. 3.

A run $\rho$ from $q \in Q$ is a valid sequence of transitions in $\langle A \rangle$ starting from $q$, of the form $\rho = q \xrightarrow{(\delta_1, a_1)} q_1 \xrightarrow{(\delta_2, a_2)} q_2 \ldots \xrightarrow{(\delta_n, a_n)} q_n$. The set of runs from $q_0$ is noted $\text{Run}(A)$ and $\text{Run}_{F_G}(A)$ denotes the subset of runs accepted by $A$, i.e. ending in a state in $F_G$. The trace of the run $\rho$ previously defined is the timed word $(l_1, a_1), (l_2, a_2) \ldots (l_n, a_n)$, with for $1 \leq i \leq n, t_i = \sum_{k=1}^{i} \delta_k$. Thus, given the trace $\sigma = (l_1, a_1), (l_2, a_2) \ldots (l_n, a_n)$ of a run $\rho$ from a state $q \in Q$ to $q' \in Q$, we can define $w = (\delta_1, a_1), (\delta_2, a_2) \ldots (\delta_n, a_n)$, with $\delta_1 = t_1$, and $\forall i \in [2, n], \delta_i = t_i - t_{i-1}$, and then $q \xrightarrow{\sigma} q'$. To ease the notation, we will only consider traces and note $q \xrightarrow{\sigma} q'$ whenever $q \xrightarrow{w} q'$ for the previously defined $w$. Note that to concatenate two traces
\( \sigma_1 \) and \( \sigma_2 \), it is needed to delay \( \sigma_2 \) to obtain a trace: the concatenation \( \sigma \) of \( \sigma_1 \) and \( \sigma_2 \) is the trace defined as \( \sigma = \sigma_1 . (\sigma_2 + 1 \times \text{time}(\sigma_1)) \). Thus, if \( q \xrightarrow{\sigma_1} q' \xrightarrow{\sigma_2} q'' \), then \( q \xrightarrow{\sigma} q'' \).

Timed Properties. A regular timed property is a timed language \( \varphi \subseteq \text{tw}(\Sigma) \) accepted by a timed automaton. For a timed word \( \sigma \), we say that \( \sigma \) satisfies \( \varphi \), noted \( \sigma \models \varphi \) whenever \( \sigma \in \varphi \). We only consider regular timed properties whose associated automaton is complete and deterministic.

Given a complete and deterministic automaton \( \mathcal{A} \) s.t. \( Q \) is the set of states of \( [\mathcal{A}] \) and \( \rightarrow \) its transition relation, and a word \( \sigma \), for \( q \in Q \), we note \( q \text{ after } \sigma = q' \), where \( q' \) is s.t. \( q \overset{\sigma}{\rightarrow} q' \). Since \( \mathcal{A} \) is complete and deterministic, there exists only one such \( q' \). We note \( \text{Reach}(\sigma) = q_0 \text{ after } \sigma \).

We extend these definitions to languages: if \( L \) is a language, \( q \text{ after } L = \bigcup_{q \in L} q \text{ after } \sigma \) and \( \text{Reach}(L) = q_0 \text{ after } L \). These definitions are valid both in the untimed and timed cases. For the timed case, we also allow to add an extra parameter to after and Reach, that represents an observation time. For \( q \in Q \), \( t \in \mathbb{R}_{\geq 0} \), and \( \sigma \in \text{tw}(\Sigma) \), \( q \text{ after } (\sigma, t) = (q, \nu + t - \text{time}((\text{obs}(\sigma, t))) \), where \( (l, \nu) = \text{after}(\text{obs}(\sigma, t)) \), and \( \text{Reach}(\sigma, t) = q_0 \text{ after } (\sigma, t) \). This allows to consider states of the semantics that are reached after the last action of the input word, by letting time elapse. In particular, note that for \( (l, \nu) \in Q \), \( (l, \nu) \text{ after } (t, t) = (l, \nu + t) \) is the state reached from \( (l, \nu) \) by letting time elapse of \( t \) units. Moreover, for \( (l, \nu) \in Q \), we note \( \text{up}(l, \nu)) = \{ (l, \nu + t) \mid t \in \mathbb{R}_{\geq 0} \} \). This definition is extended to sets of states: for \( S \subseteq Q \), \( \text{up}(S) = \bigcup_{q \in S} \text{up}(q) \). We also define a predecessor operator: for \( q \in Q \) and \( a \in \Sigma \), \( \text{Pred}_a(q) = \{ q' \in Q \mid q \text{ after } a = q \} \) for the untimed setting, and \( \text{Pred}_a(q) = \{ q' \in Q \mid q' \text{ after } (0, a) = q \} \) for the timed setting. This definition is extended to words: if \( \sigma \in \Sigma^* \) (or \( \sigma \in \text{tw}(\Sigma) \)), then \( \text{Pred}_a(q) = \{ q' \in Q \mid q' \text{ after } \sigma = q \} \).

Example 1 (Shared Data Storage). Consider the property \( \varphi_1 \) described in Fig. 3 and representing writes on a shared storage device. A more detailed description of this property is given in Section 4.3. This property is similar to \( \varphi_{\text{ex}} \) (Fig. 2), but a clock has been added to impose that writes should not occur before two time units have elapsed since the reception of the last \text{LockOff} event. Thus, the set of locations of \( \varphi_1 \) is \( L = \{ l_0, l_1, l_2, l_3 \} \), the initial location is \( l_0 \), the set of clocks is \( X = \{ x \} \), the alphabet is \( \Sigma = \{ \text{Auth, LockOn, LockOff, Write} \} \), the set of accepting locations is \( G = \{ l_1, l_2 \} \), and the set of transitions contains for instance transitions \( (l_0, \top, \text{Auth}, \emptyset, l_1) \), \( (l_2, \top, \text{Auth}, \emptyset, l_2) \), and \( (l_3, \top, \text{LockOn}, \emptyset, l_3) \), where \( \top \) is the guard that holds for every clock valuation.

Let \( Q = L \times \mathbb{R}_{\geq 0} \) be the set of states of the semantics of \( \varphi_1 \), where the clock valuations are...
replaced by the value of the unique clock $x$. Then, $\text{Reach}((2, \text{Auth})) = (l_0, 0)$ after $(2, \text{Auth}) = (l_1, 2)$, and, for example, $(l_2, 3)$ after $((2, \text{LockOff}), 4) = (l_1, 2)$, because the clock is reset when the $\text{LockOff}$ action occurs, and then $4 - 2 = 2$ time units remain to reach date 4. Also, $\text{Pred}_{\text{Write}}((l_1, 3)) = \{(l_1, 3)\}$, but, for instance, $\text{Pred}_{\text{Write}}((l_1, 1)) = \emptyset$ since the only transition labelled by $\text{Write}$ and leading to $l_1$ has guard $x \geq 2$.

3. Enforcement Monitoring of Untimed Properties

In this section, $\varphi$ is a regular property defined by an automaton $A_\varphi = \langle Q, q_0, \Sigma, \rightarrow, F \rangle$. Recall that the general scheme of an enforcement mechanism (EM) is given in Fig. 1, where $S$ represents the running system, $\sigma$ its execution, $E$ the enforcement mechanism, $\varphi$ the property to enforce, and $E(\sigma)$ the output of the enforcement mechanism, which should satisfy $\varphi$.

We consider uncontrollable events in the set $\Sigma_u \subseteq \Sigma$. These events cannot be modified by an EM, i.e. they cannot be suppressed nor buffered, so they must be output by the EM whenever they are received. Let us note $\Sigma_c = \Sigma \setminus \Sigma_u$ the set of controllable events, which can be modified by the EM. An EM can decide to buffer them to delay their emission, but it cannot suppress them (nevertheless, it can delay them endlessly, keeping their order unchanged). Thus, an EM may interleave controllable and uncontrollable events.

In this section, for $q \in Q$, we note $u\text{Pred}(q) = \bigcup_{u \in \Sigma_u} \text{Pred}_u(q)$, and we extend this definition to sets of states: for $S \subseteq Q$, $u\text{Pred}(S) = \bigcup_{q \in S} u\text{Pred}(q)$. For $S \subseteq Q$, we also note $S^c = Q \setminus S$.

3.1. Enforcement Functions and their Requirements

In this section, we consider an alphabet of actions $\Sigma$. An enforcement function is a description of the input/output behaviour of an EM. Formally, we define enforcement functions as follows:

**Definition 2** (Enforcement Function). An enforcement function is a function from $\Sigma^* \rightarrow \Sigma^*$, that is increasing on $\Sigma^*$ with respect to $\preceq$: $\forall (\sigma, \sigma') \in (\Sigma^*)^2, \sigma \preceq \sigma' \implies E(\sigma) \preceq E(\sigma')$.

An enforcement function is a function that modifies an execution, and that cannot remove events it has already output.

In the sequel, we define the requirements on an EM and express them on enforcement functions. As stated previously, an EM should ensure that the executions of a running system satisfy $\varphi$, thus its enforcement function has to be sound, meaning that its output always satisfies $\varphi$:

**Definition 3** (Soundness). An enforcement function $E : \Sigma^* \rightarrow \Sigma^*$ is sound with respect to $\varphi$ in an extension-closed set $S \subseteq \Sigma^*$ if $\forall \sigma \in S, E(\sigma) \models \varphi$.

Since there are some uncontrollable events that are only observable by the EM, receiving uncontrollable events could lead to the property not being satisfied by the output of the enforcement mechanism. Moreover, some uncontrollable sequences could lead to a state of the property that would be a non-accepting sink state, leading to the enforcement mechanism not being able to satisfy the property any further. Consequently, in Definition 3, soundness is not defined for all words in $\Sigma^*$, but in a subset $S$, since it might happen that it is impossible to ensure it from the

$\S$ This choice appeared to us as the most realistic one. Extending the notions presented in this section in order to handle enforcement mechanisms with suppression is rather simple.
initial state. Thus for an EM to be effective, \( S \) needs to be extension-closed to ensure that the property is always satisfied once it has been. If \( S \) were not extension-closed, soundness would only mean that the property is sometimes satisfied (in particular, the identity function would be sound in \( \varphi \)). In practice, there may be an initial period where the enforcement mechanism does not ensure the property (which is unavoidable), but as soon as a safe state is reached, the property becomes enforceable forever (and the property is guaranteed to hold). This approach appears to be the closest to the usual one without uncontrollable events.

The usual notion of transparency (cf. (Schneider, 2000; Ligatti et al., 2009)) states that the output of an EM is the longest prefix of the input satisfying the property. The name “transparency” stems from the fact that correct executions are left unchanged. However, because of uncontrollable events, events may be released in a different order from the one they are received. Therefore, transparency can not be ensured, and we define the weaker notion of compliance.

**Definition 4 (Compliance).** \( E \) is compliant with respect to \( \Sigma_u \) and \( \Sigma_c \), noted \( \text{compliant}(E, \Sigma_u, \Sigma_c) \), if \( \forall \sigma \in \Sigma^*, E(\sigma) \preceq_{\Sigma_c} \sigma \land E(\sigma) \in \Sigma_u \land \forall u \in \Sigma_u, E(\sigma).u \preceq E(\sigma.u) \).

Intuitively, compliance states that the EM does not change the order of the controllable events and emits uncontrollable events simultaneously with their reception, possibly followed by stored controllable events. We chose to consider enforcement mechanisms that can delay controllable events. To our opinion, it corresponds to the most common choice in practice. However, other primitives, such as deletion or reordering of controllable events could be easily considered. Using other enforcement primitives would require only few changes, especially adapting the definitions of compliance and optimality, and the construction of \( G \) (see below). When clear from the context, the partition is not mentioned: \( E \) is said to be compliant, and we note it \( \text{compliant}(E) \).

We say that a property \( \varphi \) is enforceable whenever there exists a compliant function that is sound with respect to \( \varphi \).

In addition, an enforcement mechanism should be optimal in the sense that its output sequences should be maximal while preserving soundness and compliance. In the same way we defined soundness in an extension-closed set, we define optimality as follows:

**Definition 5 (Optimality).** An enforcement function \( E : \Sigma^* \rightarrow \Sigma^* \) that is compliant with respect to \( \Sigma_u \) and \( \Sigma_c \), and sound in an extension-closed set \( S \subseteq \Sigma^* \) is optimal in \( S \) if:

\[
\forall E' : \Sigma^* \rightarrow \Sigma^*, \forall \sigma \in S, \forall a \in \Sigma, \quad (\text{compliant}(E') \land E'(\sigma) = E(\sigma) \land |E'(\sigma.a)| > |E(\sigma.a)|) \Rightarrow (\exists \sigma_u \in \Sigma_u, E'(\sigma.a.\sigma_u) \not\preceq \varphi).
\]

Intuitively, optimality states that if there exists a compliant enforcement function that outputs a longer word than an optimal enforcement function, then there must exist a sequence of uncontrollable events that would lead the output of that enforcement function to violate \( \varphi \). This would imply that this enforcement function is not sound because of \( \sigma.a.\sigma_u \). Thus, an enforcement function that outputs a longer word than an optimal enforcement function can not be sound and compliant. Since it is not always possible to satisfy the property from the beginning, this condition is restrained to an extension-closed subset of \( \Sigma^* \), as is for soundness (Definition 3).

**Example 2.** We consider a simple untimed shared storage device. After Authentication, a user can write a value only if the storage is unlocked. (Un)locking the device is decided by another entity, meaning that it is not controllable by the user. Property \( \varphi_{\text{ex}} \) (see Fig. 2) formalises the above re-
quirement. \( \varphi_{ex} \) is not enforceable if the uncontrollable alphabet is \( \{\text{LockOn}, \text{LockOff}, \text{Auth}\} \) since reading the word \( \text{LockOn} \) from \( q_0 \) leads to \( q_3 \), which is not an accepting state. However, the existence of such a word does not imply that it is impossible to enforce \( \varphi_{ex} \) for some other input words. If word \( \text{Auth} \) is read, then state \( q_1 \) is reached, and from this state, it is possible to enforce \( \varphi_{ex} \) by emitting \( \text{Write} \) only when in state \( q_1 \).

3.2. Synthesising Enforcement Functions

Example 2 shows that some input words cannot be corrected by the EM because of uncontrollable events. Nevertheless, since the received events may lead to a state from which it is possible to ensure that \( \varphi \) will be satisfied (meaning that for any events received as input, the enforcement mechanism can output a sequence that satisfies \( \varphi \)), it would then be possible to define a subset of \( \Sigma^* \) in which an enforcement function would be sound.

To be compliant, an enforcement mechanism can buffer the controllable events it has received to emit them later (i.e. after having received another events). Thus, the set of states from which an enforcement mechanism can ensure soundness, i.e. ensure it can always compute a prefix of the buffer that leads to an accepting state, whatever uncontrollable events are received, depends on its buffer. Thus, to synthesise a sound and compliant enforcement function, one needs to compute the set of words that can be emitted from a certain state with a given buffer, ensuring that an accepting state is always reachable. This set will be called \( G \), and to define it, the set of states from which the enforcement mechanism can wait some events knowing an accepting state will always be reachable should be known (this set has to be a subset of \( F \) since it is possible that no event is to be received). This set of states, which depends on the buffer, will be noted \( S \), and is defined in conjunction with another set of states, \( I \), that is used only to compute \( S \). Thus, for a buffer \( \sigma \in \Sigma_c^* \), we define the sets of states \( I(\sigma) \) and \( S(\sigma) \), that represent the states from which the enforcement mechanism can output the first event of \( \sigma \), and the states in which the enforcement mechanism can wait for another event, respectively.

**Definition 6** (\( I, S \)). Given a sequence of controllable events \( \sigma \in \Sigma_c^* \), we define the sets of states of \( \varphi \), \( I(\sigma) \) and \( S(\sigma) \) by induction as follows: \( I(\epsilon) = \emptyset \), \( S(\epsilon) = \{ q \in F \mid q_0 \in \Sigma_u^* \subseteq F \} \) and, for \( \sigma \in \Sigma_c^* \) and \( a \in \Sigma_c \),

\[
I(a.\sigma) = \text{Pred}_a(S(\sigma) \cup I(\sigma)), \\
S(\sigma.a) = S(\sigma) \cup \max_{c} \{ Y \subseteq F \mid Y \cap u\text{Pred}(Y \cup I(\sigma.a)) = \emptyset \}).
\]

Intuitively, \( S(\sigma) \) is the set of “winning” states, i.e. if an enforcement mechanism has reached a state in \( S(\sigma) \) with buffer \( \sigma \), it will always be able to reach \( F \), whatever events are received afterwards, controllable or uncontrollable. Note that since there is a possibility of not receiving any other event, \( S(\sigma) \subseteq F \), because the EM could end in any of these states, thus this condition is needed to ensure that the output of the EM satisfies the property. \( S(\sigma.a) \) is defined as the biggest subset of \( F \) such that no uncontrollable event leads outside of it or \( I(\sigma.a) \), meaning that whatever uncontrollable event is received from a state in \( S(\sigma.a) \), the state reached will be either in \( F \) (since

\* Uncontrollable events are emphasised in italics.
it will be in $S(σ.a)$ or in $I(σ.a)$. In both cases, this means that
the enforcement mechanism can reach an accepting state, whatever
uncontrollable events are received.

$I(σ)$ is the set of intermediate states, the states that can be “crossed”
while emitting a prefix of the buffer. The states in $I(σ)$ do not need
to be in $F$ since no event can be received while the
EM is in these states, because it emits all the controllable word it wishes to emit at once. $I(a.σ)$
is defined as the set of all states from which following the transition labelled by $a$ leads either
to $I(σ)$ or $S(σ)$, meaning that the EM can emit the first event of its buffer to be able to reach
an accepting state, whatever uncontrollable events are received.

Now, we can use $S$ to define $G$, the set of words that can be emitted from a state $q ∈ Q$ by an
enforcement mechanism with a buffer $σ ∈ Σ^*$.

Definition 7 (G). For $q ∈ Q$, $σ ∈ Σ^*$, $G(q, σ) = \{w ∈ Σ^*_q \mid w ⪯ σ \land q after w ∈ S(w^{-1}, σ)\}$.

Intuitively, $G(q, σ)$ is the set of words that can be output by a compliant enforcement mechanism
to ensure soundness from state $q$ with buffer $σ$. When clear from context, the parameters
could be omitted: $G$ is the value of the function for the state reached by the output of an enforce-
ment mechanism with its buffer.

Now, we use $G$ to define the functional behaviour of the enforcement mechanism.

Definition 8 (Functions $store_ϕ$, $E_ϕ$). $\parallel$ Function $store_ϕ : Σ^* → Σ^* × Σ^*$ is defined as:

\[
\begin{align*}
store_ϕ(ε) &= (ε, ε); \\
\text{for } σ ∈ Σ^* \text{ and } a ∈ Σ, \text{ let } (σ_s, σ_e) = store_ϕ(σ), \text{ then:} \\
store_ϕ(σ.a) &= \begin{cases} 
(σ_s.a, σ'_s, σ'_e) & \text{if } a ∈ Σ_u \\
(σ_s, σ'_s, σ''_e) & \text{if } a ∈ Σ_c 
\end{cases}, \quad \text{where:} \\
κ_ϕ(q, w) &= \max_ϕ(G(q, w) \cup \{ε\}), \text{ for } q ∈ Q \text{ and } w ∈ Σ^*_q, \\
σ'_s &= κ_ϕ(Reach(σ_s, a), σ_c), \quad σ'_{s} = σ'^{-1}_s.σ_c, \\
σ''_e &= κ_ϕ(Reach(σ_s), σ_c.a), \quad σ''_{s} = σ''^{-1}_s.(σ_c.a).
\end{align*}
\]

The enforcement function $E_ϕ : Σ^* → Σ^*$ is defined as $E_ϕ(σ) = \Pi_1(store_ϕ(σ))$, for any $σ ∈ Σ^*$.

Figure 4 gives a scheme of the behaviour of the enforcement function. Intuitively, $σ_s$ is the word that can be released as output, whereas
$σ_e$ is the buffer containing the events that are already read/received, but
cannot be released as output yet because they lead to an unsafe state
from which it would be possible to violate the property reading only
uncontrollable events. Upon receiving a new event $a$, the enforcement
mechanism distinguishes two cases:

\[
\begin{align*}
\text{— If } a \text{ belongs to } Σ_u, \text{ then it is output, as required by compliance. Then, the longest prefix of} \\
σ_s \text{ that satisfies } ϕ \text{ and leads to a state in } S \text{ for the associated buffer is also output.} \\
\text{— If } a \text{ is in } Σ_c, \text{ then it is added to } σ_e, \text{ and the longest prefix of this new buffer that satisfies } ϕ \\
\text{and leads to a state in } S \text{ for the associated buffer is emitted, if it exists.}
\end{align*}
\]

In both cases, $κ_ϕ$ is used to compute the longest word that can be output, that is the longest word
in $G$ for the state reached so far with the current buffer of the enforcement mechanism, or $ε$ if this

$\parallel$ $E_ϕ$ and $store_ϕ$ depend on $Σ_u$ and $Σ_c$, but we did not write it in order to lighten the notations.
set is empty. The parameters of $\kappa_\varphi$ are those which are passed to $G$. They correspond to the state reached so far by the output of the enforcement mechanism, and its current buffer, respectively.

As seen in Example 2, some properties are not enforceable, but receiving some events may lead to a state from which it is possible to enforce. Therefore, it is possible to define a set of words, called $\text{Pre}(\varphi)$, such that $E_\varphi$ is sound in $\text{Pre}(\varphi)$, as stated in Proposition 2:

**Definition 9 (Pre).** The set of input words $\text{Pre}(\varphi) \subseteq \Sigma^*$ is defined as follows:

$$\text{Pre}(\varphi) = \{\sigma \in \Sigma^* \mid G(\text{Reach}(\sigma_{\Sigma_e}), \sigma_{\Sigma_c}) \neq \emptyset\} \cdot \Sigma^*$$

Intuitively, $\text{Pre}(\varphi)$ is the set of words in which $E_\varphi$ is sound. This set is extension-closed, as required by Definition 3. In $E_\varphi$, using $S$ ensures that once $G$ is not empty, then it will never be afterwards, whatever events are received. Thus, $\text{Pre}(\varphi)$ is the set of input words such that the output of $E_\varphi$ would belong to $G$. Since $E_\varphi$ outputs only uncontrollable events until $G$ becomes non-empty, the definition of $\text{Pre}(\varphi)$ considers that the state reached is the one that is reached by omitting only the uncontrollable events of $\sigma$, and the corresponding buffer would then be the controllable events of $\sigma$.

**Example 3.** Considering property $\varphi_{\text{ex}}$ (Fig. 2), with the uncontrollable alphabet $\Sigma_u = \{\text{Auth}, \text{LockOff}, \text{LockOn}\}$, $\varphi_{\text{ex}}$ is a word of size 1). Since $E_\varphi$ outputs only uncontrollable events, say $\text{LockOff}$, is received, then $q_3$ is reached, which is a non-accepting sink state, and is thus not in $S(\epsilon)$. In order to reach a state in $S$ (i.e., $q_1$ or $q_2$), it is necessary to read $\text{Auth}$. Once $\text{Auth}$ is read, $q_1$ is reached, and from there, all uncontrollable events lead to either $q_1$ or $q_2$. The same holds true from $q_2$. Thus, it is possible to stay in the accepting states $q_1$ and $q_2$, by delaying $\text{Write}$ events when in $q_2$ until a $\text{LockOff}$ event is received. Consequently, $q_1$ and $q_2$ are in $S(\sigma)$ for all $\sigma \in \Sigma_\varphi^*$, and thus $\text{Pre}(\varphi_{\text{ex}}) = \text{Write}^* \cdot \text{Auth} \cdot \Sigma^*$, since $\text{Write}$ events can be buffered while in state $q_0$ until event $\text{Auth}$ is received, leading to $q_1 \in S(\text{Write}^*)$.

$E_\varphi$, as defined in Definition 8, is an enforcement function that is sound with respect to $\varphi$ in $\text{Pre}(\varphi)$, compliant with respect to $\Sigma_u$ and $\Sigma_u$, and optimal in $\text{Pre}(\varphi)$.

**Proposition 1.** $E_\varphi$ as defined in Definition 8 is an enforcement function.

**Sketch of proof.** We have to show that for all $\sigma$ and $\sigma' \in \Sigma^*$, $E_\varphi(\sigma) \preceq E_\varphi(\sigma')$. Following the definition of $\text{store}_\varphi$, this holds provided that $\sigma' \in \Sigma$ (i.e., $\sigma'$ is a word of size 1). Since $\preceq$ is an order, it follows that the proposition holds for all $\sigma' \in \Sigma^*$.

**Proposition 2.** $E_\varphi$ is sound with respect to $\varphi$ in $\text{Pre}(\varphi)$, as per Definition 3.

**Sketch of proof.** We have to show that if $\sigma \in \text{Pre}(\varphi)$, then $E_\varphi(\sigma) \models \varphi$. The proof is made by induction on $\sigma$. In the induction step, considering $a \in \Sigma$, we distinguish three different cases:

— $\sigma.a \notin \text{Pre}(\varphi)$. Then the proposition holds.
— $\sigma.a \in \text{Pre}(\varphi)$, but $\sigma \notin \text{Pre}(\varphi)$. Then the input reaches $\text{Pre}(\varphi)$, and since it is extension-closed, all extensions of $\sigma$ also are in $\text{Pre}(\varphi)$, and we prove that the proposition holds considering the definition of $\text{Pre}(\varphi)$.
— $\sigma \in \text{Pre}(\varphi)$ (and thus, $\sigma.a \in \text{Pre}(\varphi)$ since it is extension-closed). Then, we prove that the proposition holds, based on the definition of $\text{store}_\varphi$, and more precisely on the definition of $S$, that ensures that there always exists a compliant output that satisfies $\varphi$.

**Proposition 3.** $E_\varphi$ is compliant, as per Definition 4.
Figure 5: Property that can be enforced by blocking all controllable events $c$.

**Sketch of proof.** The proof is made by induction on the input $\sigma \in \Sigma^*$. Considering $\sigma \in \Sigma^*$ and $a \in \Sigma$, the proof is straightforward by considering the different values of $store_\varphi(\sigma.a)$, $(\sigma.a)_{\Sigma_u}$, and $(\sigma.a)_{\Sigma_c}$ when $a \in \Sigma_c$ and $a \in \Sigma_u$.

**Remark 2.** Notice that for some properties, an enforcement function that would block all controllable events may still be sound and compliant. Consider for instance the property represented in Fig. 5, where $c$ is a controllable event, and $u$ an uncontrollable event. Then, outputting only the events $u$ and buffering all the $c$ events allows to stay in state $q_0$, which is accepting and in $S(\sigma)$ for every word $\sigma \in c^*$. This means that an enforcement mechanism that blocks all controllable events would be sound and compliant. Nevertheless, if two controllable events $c$ are received, they can be output to reach state $q_2$, which is also accepting and safe for all possible sequences. Then it is possible to release more events. Therefore, an enforcement mechanism that would output two $c$ events when they are received would be “better” than the first one blocking all of them, in the sense that its output would be longer (and thus closer to the input).

For any $\sigma \in \text{Pre}(\varphi)$, $E_{\varphi}(\sigma)$ is the longest possible word that ensures soundness and compliance, that is controllable events are blocked only when necessary. Thus, $E_{\varphi}$ is also optimal in $\text{Pre}(\varphi)$:

**Proposition 4.** $E_{\varphi}$ is optimal in $\text{Pre}(\varphi)$, as per Definition 5.

**Sketch of proof.** The proof is made by induction on the input $\sigma \in \Sigma^*$. Once $\sigma \in \text{Pre}(\varphi)$, we know that $E_{\varphi}(\sigma) \models \varphi$ since $E_{\varphi}$ is sound in $\text{Pre}(\varphi)$. $E_{\varphi}$ is optimal because in $\text{store}_\varphi$, $\kappa_{\varphi}$ provides the longest possible word. If a longer word were output, then either the output would not satisfy $\varphi$, or it would lead to a state that is not in $S$ for the corresponding buffer, meaning that there would exist an uncontrollable word leading to a non-accepting state that would not be in $S$ for the buffer. Then, the enforcement mechanism would have to output some controllable events from the buffer to reach an accepting state, but since the state is not in $S$, there would exist again an uncontrollable word leading to a non-accepting state that is not in $S$ for the updated buffer. By iterating, the buffer would become $\epsilon$ whereas the output of the enforcement mechanism would be leading to a non-accepting state. Therefore, outputting a longer word would mean that the function is not sound. This means that $E_{\varphi}$ is optimal in $\text{Pre}(\varphi)$, since it outputs the longest word that allows to be both sound and compliant.

**Example 4.** Consider property $\varphi_{ex}$ (Fig. 2). We illustrate in table 1 the enforcement mechanism by showing the evolution of $\sigma_s$ and $\sigma_c$ with input $\sigma = \text{Auth.LockOn.Write.LockOff}$.

### 3.3. Enforcement Monitors

Enforcement monitors are operational descriptions of EMs. We give a representation of an EM for a property $\varphi$ as an input/output transition system. The input/output behaviour of the enforce-
Table 1: Example of the evolution of \((\sigma_s, \sigma_c) = \text{store}_{\varphi}(\sigma)\), with input \(\text{Auth.LockOn.Write.LockOff}\)

<table>
<thead>
<tr>
<th>(\sigma)</th>
<th>(\sigma_s)</th>
<th>(\sigma_c)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\varepsilon)</td>
<td>(\varepsilon)</td>
<td>(\varepsilon)</td>
</tr>
<tr>
<td>(\text{Auth})</td>
<td>(\text{Auth})</td>
<td>(\varepsilon)</td>
</tr>
<tr>
<td>(\text{Auth.LockOn})</td>
<td>(\text{Auth.LockOn})</td>
<td>(\varepsilon)</td>
</tr>
<tr>
<td>(\text{Auth.LockOn.Write})</td>
<td>(\text{Auth.LockOn})</td>
<td>(\text{Write})</td>
</tr>
<tr>
<td>(\text{Auth.LockOn.Write.LockOff})</td>
<td>(\text{Auth.LockOn.LockOff.Write})</td>
<td>(\varepsilon)</td>
</tr>
</tbody>
</table>

---

**Definition 10 (Enforcement Monitor).** An enforcement monitor \(E\) for \(\varphi\) is a transition system \((C^E, c^E_0, \Gamma^E, \rightarrow^E)\) such that:

- \(C^E = Q \times \Sigma^*\) is the set of configurations.
- \(c^E_0 = (q_0, \varepsilon)\) is the initial configuration.
- \(\Gamma^E = \Sigma^* \times \{\text{dump}(), \text{pass-uncont}(), \text{store-cont}()\} \times \Sigma^*\) is the alphabet, where the first, second, and third members are an input sequence, an enforcement operation, and an output sequence, respectively.
- \(\rightarrow^E \subseteq C^E \times \Gamma^E \times C^E\) is the transition relation, defined as the smallest relation obtained by applying the following rules in order (where \(w/\vartriangleleft w'\) stands for \((w, \vartriangleleft, w') \in \Gamma^E\)):
  - **Dump**: \(\langle q, a.c, \epsilon \rangle \xrightarrow{\text{dump}(a)/\epsilon} \langle q', \sigma_c \rangle\), if \(a \in \Sigma_c\), \(G(q, a.c) \neq \emptyset\) and \(G(q, a.c) \neq \{\epsilon\}\), with \(q' = q\) after \(a\),
  - **Pass-uncont**: \(\langle q, \sigma_c \rangle \xrightarrow{a/\text{pass-uncont}(a)/\epsilon} \langle q', \sigma_c \rangle\), with \(a \in \Sigma_a\) and \(q' = q\) after \(a\),
  - **Store-cont**: \(\langle q, \sigma_c \rangle \xrightarrow{a/\text{store-cont}(a)/\epsilon} \langle q, \sigma_c, a \rangle\), with \(a \in \Sigma_c\).

In \(E\), a configuration \(c = \langle q, \sigma \rangle\) represents the current state of the enforcement mechanism. The state \(q\) is the one reached so far in \(A_\varphi\) with the output of the monitor. The word of controllable events \(\sigma_c\) represents the buffer of the monitor, i.e. the controllable events of the input that it has not output yet. Rule **dump** outputs the first event of the buffer if it can ensure soundness afterwards (i.e. if there is a non-empty word in \(G\), that must begin with this event). Rule **pass-uncont** releases an uncontrollable event as soon as it is received. Rule **store-cont** simply adds a controllable event at the end of the buffer. Compared to Section 3.2, the second member of the configuration represents buffer \(\sigma_c\) in the definition of \(\text{store}_\varphi\), whereas \(\sigma_s\) is here represented by state \(q\) which is the first member of the configuration, such that \(q = \text{Reach}(\sigma_s)\).

**Proposition 5.** The output of the enforcement monitor \(E\) for input \(\sigma\) is \(E_\varphi(\sigma)\).

In Proposition 5, the output of the enforcement monitor is the concatenation of all the outputs of the word labelling the path followed when reading \(\sigma\). A more formal definition is given in the proof of this proposition, in appendix A.1.

**Sketch of proof.** The proof is made by induction on the input \(\sigma \in \Sigma^*\). We consider the rules applied when receiving a new event. If the event is controllable, then rule **store-cont()** can be applied, possibly followed by rule **dump()** applied several times. If the event is uncontrollable, then rule **pass-uncont()** can be applied, again possibly followed by rule **dump()** applied several times.
times. Since rule dump() applies only when there is a non-empty word in G, then this word must begin with the first event of the buffer, and the rule dump() can be applied again if there was a word in G of size at least 2, meaning that there is another non-empty word in the new set G, and so on. Thus, the output of all the applications of the rule dump() corresponds to the computation of \( \kappa_\varphi \) in the definition of store_\varphi, and consequently the outputs of E and E_\varphi are the same.

**Remark 3.** Enforcement monitors as per Definition 10 are somewhat similar to the configuration description of EMs in (Falcone et al., 2011). The main difference with the EMs considered in (Falcone et al., 2011) is that the rule to be applied depends on the memory (the buffer), whereas in (Falcone et al., 2011) it only depends on the state and the event received.

### 4. Enforcement Monitoring of Timed Properties

We extend the framework in Section 3 to enforce timed properties. EMs and their properties need to be redefined to fit with timed properties. Enforcement functions need an extra parameter representing the date at which the output is observed. Soundness needs to be weakened so that, at any time instant, the property is allowed not to hold, provided that it will hold in the future.

Considering uncontrollable events with timed properties raises several difficulties. First, as in the untimed case, the order of events might be modified. Thus, previous definitions of transparency (Pinsent et al., 2012), stating that the output of an enforcement function will eventually be a delayed prefix of the input, can not be used in this situation. Moreover, when delaying some events to have the property satisfied in the future, one must consider the fact that some uncontrollable events could occur at any moment (and cannot be delayed). Finally, some properties become not enforceable because of uncontrollable events, meaning that for these properties it is impossible to obtain sound EMs, as shown in Example 5.

In this section, \( \varphi \) is a timed property defined by a timed automaton \( A_\varphi = \langle Q, l_0, X, \Sigma, \Delta, G \rangle \) with semantics \( [A_\varphi] = \langle Q, q_0, \Gamma, \rightarrow, F_G \rangle \). As in the untimed setting, for \( q \in Q \), we define \( uPred(q) = \bigcup_{u \in \Sigma_u} Prod_u(q) \), and for \( S \subseteq Q \), \( uPred(S) = \bigcup_{q \in S} uPred(q) \) and \( S = Q \setminus S \).

**Example 5 (Non-Enforceable Property).** Consider the property defined by the automaton in Fig. 6 with alphabet \{a, b\}. If all actions are controllable (\( \Sigma_u = \emptyset \)), the property is enforceable because of uncontrollable events, meaning that for these properties it is impossible to obtain sound EMs, as shown in Example 5.

4.1. Enforcement Functions and their Properties

An enforcement function takes a timed word and the current time as input, and outputs a timed word:

**Definition 11 (Enforcement Function).** Given an alphabet of actions \( \Sigma \), an enforcement function is a function \( E : tw(\Sigma) \times \mathbb{R}_{\geq 0} \rightarrow tw(\Sigma) \) s.t.:  

\[
\forall \sigma \in tw(\Sigma), \forall t \in \mathbb{R}_{\geq 0}, \forall t' \geq t, \quad E(\sigma, t) \preceq E(\sigma, t') \quad \land \quad (\sigma.(t,a) \in tw(\Sigma) \implies E(\sigma, t) \preceq E(\sigma.(t,a), t)).
\]
Definition 11 models physical constraints: an enforcement function can not remove something already output. The two conditions correspond to letting time elapse and reading a new event, respectively. In both cases, the new output must be an extension of what has been output so far.

**Soundness** states that the output of an enforcement function should eventually satisfy the property:

**Definition 12 (Soundness).** An enforcement function $E$ is *sound* with respect to $\varphi$ in a time-extension-closed set $S \subseteq \text{tw}(\Sigma) \times \mathbb{R}_{\geq 0}$ if $\forall (\sigma, t) \in S, \exists ! t' \geq t, \forall t'' \geq t', E(\sigma, t'') \models \varphi$.

An enforcement function is sound in a time-extension-closed set $S$ if for any $(\sigma, t)$ in $S$, the value of the enforcement function with input $\sigma$ from date $t$ satisfies the property in the future. As in the untimed setting, soundness is not defined for all words in $\text{tw}(\Sigma)$, but in a set of words, this time associated with dates. The reason is the same as in the untimed setting: the EM might not be able to ensure soundness from the beginning, because of bad uncontrollable sequences. Moreover, in the definition of soundness, the set $S$ needs to be time-extension-closed to ensure that the property remains satisfied once the EM starts to operate.

**Remark.** Soundness could have been defined in the same way as in the untimed setting, however, with such alternative stronger definition, where the output of the EM must always satisfy the property, less properties could be enforced. Weakening soundness allows to enforce more properties, and to let enforcement mechanisms produce longer outputs.

**Compliance** states that uncontrollable events should be emitted instantaneously upon reception, and that controllable events can be delayed, but their order must remain unchanged:

**Definition 13 (Compliance).** Given an enforcement function $E$ defined on an alphabet $\Sigma$, we say that $E$ is *compliant* with respect to $\Sigma_u$ and $\Sigma_c$, noted compliant($E, \Sigma_u, \Sigma_c$), if $\forall \sigma \in \text{tw}(\Sigma), \forall t \in \mathbb{R}_{\geq 0}, E(\sigma, t) \preceq_{\Sigma_c} \sigma \land E(\sigma, t) =_{\Sigma_u} \text{obs}(\sigma, t) \land \forall u \in \Sigma_u, E(\sigma, t), (t, u) \not\preceq E(\sigma, (t, u), t)$.

Compliance is similar to the one in the untimed setting except that the controllable events can be delayed. However, their order must not be modified by the EM, that is, when considering the projections on controllable events, the output should be a delayed prefix of the input. Any uncontrollable event is released immediately when received, that is, when considering the projections on uncontrollable events, the output should be equal to the input.

We say that a property is *enforceable* whenever there exists a sound and compliant enforcement function for this property.

For a compliant enforcement function $E : \text{tw}(\Sigma) \times \mathbb{R}_{\geq 0} \rightarrow \text{tw}(\Sigma)$, and a timed word $\sigma \in \text{tw}(\Sigma)$, we note $E(\sigma)$ the value of $E$ with input $\sigma$ at infinite time (i.e. when it has stabilised). More formally, $E(\sigma) = E(\sigma, t)$, where $t \in \mathbb{R}_{\geq 0}$ is s.t. for all $t' \geq t$, $E(\sigma, t') = E(\sigma, t)$. Since $\sigma$ is finite, and $E$ is compliant, the output of $E$ with input word $\sigma$ is finite, thus such a $t$ must exist.

As in the untimed setting, we define a notion of **optimality** in a set:

**Definition 14 (Optimality).** We say that an enforcement function $E : \text{tw}(\Sigma) \times \mathbb{R}_{\geq 0} \rightarrow \text{tw}(\Sigma)$ that is compliant with respect to $\Sigma_c$ and $\Sigma_u$ and sound in a time-extension-closed set $S \subseteq \text{tw}(\Sigma) \times \mathbb{R}_{\geq 0}$ is *optimal* in $S$ if for any enforcement function $E' : \text{tw}(\Sigma) \times \mathbb{R}_{\geq 0} \rightarrow \text{tw}(\Sigma)$, for all $\sigma \in \text{tw}(\Sigma),$ for all $(t, a) \in \text{tw}(\Sigma)$,

\[
\text{compliant}(E', \Sigma_u, \Sigma_c) \land (\sigma, t) \in S \land E'(\sigma, t) = E(\sigma, t) \land E(\sigma, (t, a)) \not\preceq_d E'(\sigma, (t, a))
\implies (\exists \sigma_u \in \text{tw}(\Sigma_u), E'(\sigma, (t, a), \sigma_u) \not\models \varphi).
\]

Optimality states that outputting a greater word (with respect to $\preceq_d$) than the output of an
optimal enforcement function leads to either compliance or soundness not being guaranteed. This holds from the point where the input begins to belong to the set in which the function is optimal, and since it is time-extension-closed, the input will belong to this set afterwards. In Definition 14, $E$ is an optimal enforcement function, and $E'$ is another compliant enforcement function, that we consider having a greater output (with respect to $\leq_\varphi$) than $E$ for some input word $\sigma.(t, a)$. Then, since $E$ is optimal, $E'$ is not sound, because there exists a word of uncontrollable events s.t. the output of $E'$ after receiving it eventually violates $\varphi$.

An EM delaying events should buffer them until it can output them. Being able to enforce $\varphi$ depends on the possibility of computing a timed word with the events of the buffer, even when receiving some uncontrollable events, that leads to an accepting state from the current one. Thus, we define, for every sequence $\sigma$ of controllable actions, two sets of states of the semantics of $A_\varphi$, $S(\sigma)$ and $I(\sigma)$. $S(\sigma)$ is the largest set s.t. from any of its states, it is possible to wait before emitting a word that leads to $F_G$, knowing that all along the path, receiving an uncontrollable event will not prevent from computing such a word again. $I(\sigma)$ is the set of states from which it is possible to emit the first event of $\sigma$ and reach a state from which it is possible to compute a word that leads to $F_G$, again s.t. receiving uncontrollable events does not prevent from eventually reaching $F_G$.

**Definition 15** (I, S). The sets of states of $[A_\varphi]$, $I(\sigma)$ and $S(\sigma)$, are inductively defined over sequences of controllable events as follows: $I(\epsilon) = \emptyset$ and $S(\sigma) = \{ q \in F_G \mid q \text{ after } tw(\Sigma_u) \subseteq F_G \}$ and, for $\sigma \in \Sigma_\epsilon^*$ and $a \in \Sigma_c$,

\[
I(a.\sigma) = \text{Pred}_q(I(\sigma) \cup S(\sigma)),
\]

\[
S(\sigma.a) = S(\sigma) \cup \max_{\leq}\{X \cup Y \subseteq Q \mid Y \subseteq F_G \land Y = \text{up}(Y) \land (\forall x \in X, \exists i \in I(\sigma.a), \exists \delta \in \mathbb{R}_{\geq 0}, x \text{ after } (\epsilon, \delta) = i \land \forall t < \delta, x \text{ after } (\epsilon, t) \in X) \land (X \cup Y) \cap \text{upred}(X \cup Y \cup I(\sigma.a)) = \emptyset\}
\]

Intuitively, in Definition 15, $S(\sigma)$ is the set of states of the semantics of $\varphi$ that our EM will be allowed to reach with a buffer $\sigma$. It corresponds to the states from which the EM will be able to reach $F_G$, meaning that its output will satisfy the property, even if some uncontrollable events are received. From any state in $S(\sigma)$, the EM can compute a word of controllable events (taken from its buffer $\sigma$) leading to $F_G$, and if some uncontrollable events are received, it will also be able to compute a new word to reach $F_G$, with events taken from its (possibly modified due to previous emissions of events) buffer. The set $I(\sigma)$ is the set of states that the output of the enforcement mechanism will be authorised to “traverse”, meaning that the enforcement mechanism can emit the first event of its buffer $\sigma$ immediately from these states, but not wait in them (contrary to the states in $S(\sigma)$, from which the EM could choose to wait before emitting a new event).

These sets are defined by induction on $\sigma$, which represents the buffer of the EM. If the EM has its buffer empty ($\sigma = \epsilon$), then the set of states from which it can emit a controllable event is empty, since it can only emit events from its buffer: $I(\epsilon) = \emptyset$. Nevertheless, some states in $F_G$ can be s.t. all uncontrollable words lead to a state in $F_G$, meaning that from these states, the property will be satisfied even if some uncontrollable events are received. Consequently, $S(\epsilon) = \{ q \in F_G \mid q \text{ after } tw(\Sigma_u) \subseteq F_G \}$. 

\[
\]
If a new controllable event $a$ is received, it is added to the buffer, and then the EM can decide to emit the first event of its buffer to reach a state that is in $S$ or $I$ for its new buffer, this explains the definition of $I(a, \sigma)$. Adding a new event to the buffer gives more possibilities to the EM (since it could act as if it had not received this event), thus $S(\sigma) \subseteq S(\sigma a)$. Moreover, $S(\sigma a)$ is made of the union of two sets, $X$ and $Y$. $X$ is the set of states from which the EM can decide to wait before emitting the first event of its buffer, thus waiting from a state of $X$ has to lead to a state in $I(\sigma a)$. $Y$ is the set of states that are in $F_G$ and from which the EM can decide to wait for a new uncontrollable event before doing anything. Since $Y \subseteq F_G$, if no uncontrollable event is to be received, the property is satisfied, and otherwise, the EM can decide what to emit to reach $F_G$. In order to ensure that receiving uncontrollable events do not prevent from being able to reach $F_G$ with events from the buffer, $X$ and $Y$ are s.t. every uncontrollable event received from a state in $X$ or $Y$ leads to a state in $X$, $Y$, or $I(\sigma a)$. This is the purpose of the condition $(X \cup Y) \cap \text{uPred}(X \cup Y \cup I(\sigma a)) = \emptyset$. On top of this, it is necessary to ensure that all the states reached while waiting from $X$ or $Y$ are in $X$ or $Y$, otherwise there could be a state reached by the EM for which there is an uncontrollable event leading to a state from which it is impossible to reach $F_G$ with events of the buffer, meaning that the enforcement would not be sound. This is ensured by the conditions $x$ after $(\epsilon, t) \in X$, and $Y = \text{up}(Y)$. To have the best EM possible, these sets are as large as possible.

Note that if $X_1$ and $X_2$ satisfy the conditions required for $X$, then $X_1 \cup X_2$ also satisfies them. Thus, the bigger set satisfying these properties exists. The same holds for $Y$.

For convenience, we also define $G : Q \times \Sigma_c \to 2^{\text{tw}(\Sigma)}$ which gives, for a state $q$ and a sequence of controllable events $\sigma$, the set of timed words made with the actions of $\sigma$ that can be output from $q$ in a safe way (i.e. all the states reached while emitting the word are in the $S$ set corresponding to what remains from $\sigma$):

$$G(q, \sigma) = \{ w \in \text{tw}(\Sigma) \mid \Pi_\Sigma(w) \not\subseteq \sigma \land q \text{ after } w \in F_G \land \forall t \in \mathbb{R}_{\geq 0}, q \text{ after } (w, t) \in S(\Pi_\Sigma(\text{obs}(w, t))^{-1}, \sigma)\}.$$ 

It is now possible to use $G$ to define an enforcement function for $\varphi$, denoted as $E_\varphi$:

**Definition 16** (Functions $\text{store}_\varphi, E_\varphi$). Let $\text{store}_\varphi$ be the function : $\text{tw}(\Sigma) \times \mathbb{R}_{\geq 0} \to \text{tw}(\Sigma) \times \text{tw}(\Sigma_c) \times \Sigma_c^*$ defined inductively by:

$$\forall t \in \mathbb{R}_{\geq 0}, \text{store}_\varphi(\epsilon, t) = (\epsilon, \epsilon, \epsilon),$$

and for $\sigma \in \text{tw}(\Sigma), (t', a) \in \text{tw}(\Sigma)$, and $t \geq t'$, if $(\sigma_s, \sigma_b, \sigma_c) = \text{store}_\varphi(\sigma, t')$, then

$$\text{store}_\varphi(\sigma, (t', a), t) = \begin{cases} (\sigma_s, (t', a), \text{obs}(\sigma'_b, t), \sigma'_c) & \text{if } a \in \Sigma_u \\ (\sigma_s, \text{obs}(\sigma''_b, t), \sigma''_c, \sigma''_c) & \text{if } a \in \Sigma_c \end{cases}$$

with:

$$\kappa_\varphi(q, w) = \min_{\text{lex}}(\max(G(q, w) \cup \{\epsilon\})), \text{ for } q \in Q \text{ and } w \in \Sigma_c^*,$$

$$\text{buffer}_c = \Pi_\Sigma(\text{obs}(\sigma_b, t)), \sigma_c,$$

$$t_1 = \min\{t'' \in \mathbb{R}_{\geq 0} \mid t'' \geq t' \land G(\text{Reach}(\sigma_s, (t', a), t''), \text{buffer}_c) \neq \emptyset \cup \{\infty\}\},$$

$$\sigma'_b = \kappa_\varphi(\text{Reach}(\sigma_s, (t', a), \min\{t, t_1\}), \text{buffer}_c),$$

$$\sigma'_c = \Pi_\Sigma(\sigma'_b)^{-1}. \text{buffer}_c,$$
\[ t_2 = \min\{t'' \in \mathbb{R}_{\geq 0} \mid t'' \geq t' \land \]
\[ G(\text{Reach}(\sigma_s, t''), \text{buffer}_c, a) \neq \emptyset \} \cup \{+\infty\}, \]
\[ \sigma''_b = \kappa_\varphi(\text{Reach}(\sigma_s, \min(\{t, t_2\})), \text{buffer}_c, a) +_1 \min(\{t, t_2\}), \]
\[ \sigma''_c = \Pi_\Sigma(\sigma''_b)^{-1}(\text{buffer}_c, a). \]

For \( \sigma \in \text{tw}(\Sigma) \), and \( t \in \mathbb{R}_{\geq 0} \), we define \( E_\varphi(\sigma, t) = (\Pi_1(\text{store}_\varphi(\text{obs}(\sigma, t), t))). \)

The function \( \text{store}_\varphi \) takes a timed word \( \sigma \) and a date \( t \) as input, and outputs three words: \( \sigma_s, \sigma_b, \) and \( \sigma_c. \) \( \sigma_s \) is the output of the enforcement function at time \( t. \) \( \sigma_b \) is the timed word, composed of controllable events, that is to be output after the date of the last event of the input, if no uncontrollable event is received. \( \sigma_c \) is the untimed word composed of the remaining controllable actions of the buffer. When time elapses, after the last event of the input, \( \sigma_s \) is modified to output the events of \( \sigma_b \) when the dates are reached. Since letting time elapse can disable some transitions, it is possible to reach a state in \( S \) or \( I \) without emitting any event, and thus \( \sigma_b \) can change at this moment, changing from \( \epsilon \) to a word in \( G. \) This change of \( \sigma_b \) when letting time elapse can only happen once, since \( G \) will not be empty anymore once it has become non-empty. \( t_1 \) and \( t_2 \) are used for this purpose, they both represent the time at which \( G \) becomes non-empty, if \( a \in \Sigma_u \) or \( a \in \Sigma_c \) respectively. Words are thus calculated from this point whenever \( G \) has become non-empty, to ensure that what has already been output is not modified. If \( G \) is still empty, then \( \min(\{t, t_1\}) \) or \( \min(\{t, t_2\}) \), depending on whether \( a \in \Sigma_c \) or \( a \in \Sigma_u \) equals to \( t, \) meaning that \( \sigma_b = \epsilon. \) Most of the time, \( t_1 \) or \( t_2 \) is equal to \( t', \) it is not the case only when \( G \) was still empty at time \( t', \) but if \( G \) was not empty at date \( t', \) then \( t_1 \) or \( t_2 \) is equal to \( t'. \) \( \sigma_c \) contains the controllable actions of the input that have not been output and do not belong to \( \sigma_b. \)

It is used to compute the new value of \( \sigma_b \) when possible. When receiving a new event in the input, it is appended to \( \sigma_s \) if it is an uncontrollable event, or the action is appended to the buffer if it is a controllable one. Then, \( \sigma_b \) is computed again, from the new state reached if it was an uncontrollable event, or with the new buffer if it was controllable. Note that \( t_1 \) and \( t_2 \) may not exist, since they are minima of an interval that can be open, depending on the strictness of the considered guard. In this case, one should consider the infimum instead of the minimum, and add an infinitesimal delay, s.t. the required transition is taken.

As mentioned previously, an EM may not be sound from the beginning of an execution, but some uncontrollable events may lead to a state from which it becomes possible to be sound. Whenever \( \sigma_0 \) is in \( G, \) then it will always be, meaning that the output of \( E_\varphi \) will eventually reach a state in \( F_G, \) i.e. it will eventually satisfy \( \varphi. \) Thus, \( E_\varphi \) eventually satisfies \( \varphi \) as soon as the state reached so far is in \( S(\sigma_0) \) or \( I(\sigma_0). \) This leads to the definition of \( \text{Pre}(\varphi, t) \), which is the set of timed words for which \( E_\varphi \) ensures soundness at time \( t. \) For \( \sigma \in \text{tw}(\Sigma), \) if \( (\sigma_s, \sigma_b, \sigma_c) = \text{store}_\varphi(\sigma, t), \) then \( \sigma \) is in \( \text{Pre}(\varphi, t) \) if and only if the set \( G(\text{Reach}(\sigma_s, t), \Pi_\Sigma(\text{nobs}(\sigma_b, t)), \sigma_c) \) is not empty. Then, \( \text{Pre}(\varphi, t) \) is used to define \( \text{Pre}(\varphi), \) which is the set in which \( E_\varphi \) is sound:

**Definition 17 (\( \text{Pre}(\varphi) \)).** \( \text{Pre}(\varphi) = \{(\sigma, t) \mid \sigma \in \text{Pre}(\varphi, t)\}, \) where, for \( \sigma \in \text{tw}(\Sigma) \) and \( t \in \mathbb{R}_{\geq 0}. \)

\[ \text{Pre}(\varphi, t) = \{\sigma \in \text{tw}(\Sigma) \mid \exists \sigma' \preceq \sigma, \exists t' \leq t, \]
\[ G(\text{Reach}(\sigma', t'|_\Sigma, t'), \Pi_\Sigma(\text{nobs}(\sigma'(t)|_\Sigma))) \neq \emptyset\}. \]

Note that \( \text{Pre}(\varphi) \) is time-extension-closed, meaning that once \( E_\varphi \) is sound, its output will always eventually satisfy \( \varphi \) in the future.

Since the output of our enforcement function consists only of the uncontrollable events from
the input, if \( G(\text{Reach}(\text{obs}(\sigma, t)_{\Sigma}, t), \Pi_{\Sigma}(\text{obs}(\sigma, t)_{\Sigma})) \) is not empty, this means that the enforcement function becomes sound with input \( \sigma \) from time \( t \), since there is a word that is safe to emit. Thus, \( \text{Pre}(\varphi, t) \) is the set of inputs for which \( E_\varphi \) is sound after date \( t \), and then \( E_\varphi \) is sound for any input in \( \text{Pre}(\varphi) \) after its associated date.

**Proposition 6.** \( E_\varphi \) as defined in Definition 16 is an enforcement function, as per Definition 11.

**Sketch of proof.** We have to show that for all \( \sigma \in \text{tw}(\Sigma) \), for all \( t \in \mathbb{R}_{\geq 0} \) and \( t' \geq t \), \( E_\varphi(\sigma, t) \preceq E_\varphi(\sigma, t') \), and for all \( (t, a) \) s.t. \( \sigma(t, a) \in \text{tw}(\Sigma) \), \( E_\varphi(\sigma, t) \preceq E_\varphi(\sigma(t, a), t) \). To prove this, we first show by induction that \( E_\varphi(\sigma, t) \preceq E_\varphi(\sigma, t') \). Considering \( (t'', a) \) s.t. \( \sigma(t'', a) \in \text{tw}(\Sigma) \), we distinguish different cases according to the values of \( t'' \) compared to \( t \) and \( t' \):

- \( t'' \leq t \). Then, in the definition of \( \text{store}_\varphi, t_1 \) (or \( t_2 \), if \( a \) is controllable) has the same value in \( \text{store}_\varphi(\sigma, t) \) and \( \text{store}_\varphi(\sigma(t'', a), t') \). Then, comparing \( t \) to \( t_1 \), either \( E_\varphi(\sigma(t'', a), t) = \epsilon \) if \( t < t_1 \), and then \( E_\varphi(\sigma(t'' \cdot a), t) \not\preceq E_\varphi(\sigma(t'', a), t') \), or \( t \geq t_1 \), and then there exists \( \sigma_b \) s.t. \( E_\varphi(\sigma(t'', a), t) = \sigma \cdot \text{obs}(\sigma_b, t) \) and \( E_\varphi(\sigma(t'', a), t') = \sigma \cdot \text{obs}(\sigma_b, t') \), meaning that \( E_\varphi(\sigma(\sigma(t'', a), t) \not\preceq E_\varphi(\sigma(t'', a), t') \).

- \( t'' > t \). Then the proposition holds because in the definition of \( E_\varphi \), only the observation of the input word at the given time is considered, meaning that \( E_\varphi(\sigma(t'', a), t) = \sigma \cdot \text{obs}(\sigma_b, t) \) and \( E_\varphi(\sigma(t'', a), t') = \sigma \cdot \text{obs}(\sigma_b, t') \). By induction hypothesis, the proposition thus holds.

- \( t < t'' < t' \). Then, \( E_\varphi(\sigma(t'', a), t) = E_\varphi(\sigma(t'', a), t') \), and \( E_\varphi(\sigma(t'', a), t') = \Pi_{\text{store}_\varphi}(\sigma(t'', a), t') \), meaning that, looking at the definition of \( \text{store}_\varphi \), \( E_\varphi(\sigma(t'', a), t) \not\preceq E_\varphi(\sigma(t'', a), t') \).

Thus, \( E_\varphi(\sigma, t) \not\preceq E_\varphi(\sigma, t') \). Then, what remains to show is that if \( \sigma(t, a) \in \text{tw}(\Sigma) \), then \( E_\varphi(\sigma(t, a), t) \not\preceq E_\varphi(\sigma(t, a), t) \). Following the definition of \( \text{store}_\varphi \), it is clear that \( \text{store}_\varphi(\sigma(t, a), t) \not\preceq \text{store}_\varphi(\sigma(t, a), t) \), and thus \( E_\varphi(\sigma(t, a), t) \not\preceq E_\varphi(\sigma(t, a), t) \).

**Proposition 7.** \( E_\varphi \) is sound with respect to \( \varphi \) in \( \text{Pre}(\varphi) \) as per Definition 12.

**Sketch of proof.** As in the untimed setting, the proof is made by induction on the input \( \sigma \in \text{tw}(\Sigma) \). Similarly to the untimed setting, considering \( \sigma \in \text{tw}(\Sigma) \), \( t \in \mathbb{R}_{\geq 0} \), and \( (t', a) \) s.t. \( \sigma(t', a) \in \text{tw}(\Sigma) \), there are three possibilities:

- \( \sigma(t', a), t \not\in \text{Pre}(\varphi) \). Then, the proposition holds.
- \( \sigma(t', a), t \in \text{Pre}(\varphi) \), but \( \sigma(t') \not\in \text{Pre}(\varphi) \). Then, this is when the input reaches \( \text{Pre}(\varphi) \).

Considering the definition of \( \text{Pre}(\varphi) \), we then prove that it is possible to emit a word with the controllable events seen so far, leading to an accepting state in \( S \).

- \( (\sigma, t') \in \text{Pre}(\varphi) \) (and thus \( \sigma(t', a), t \) too). Then, we prove again that there exists a controllable word made with the events which have not been output yet leading to an accepting state that is in \( S \), but this time considering the definitions of \( S \) and 1.

**Proposition 8.** \( E_\varphi \) is compliant, as per Definition 13.

**Sketch of proof.** As in the untimed setting, the proof is made by induction on the input \( \sigma \), considering the different cases where the new event is controllable or uncontrollable. The only difference with the untimed setting is that one should consider dates on top of actions.

**Proposition 9.** \( E_\varphi \) is optimal in \( \text{Pre}(\varphi) \), as per Definition 14.

**Sketch of proof.** This proof is made by induction on the input \( \sigma \). Whenever \( \sigma \in \text{Pre}(\varphi) \), since \( E_\varphi \) is sound in \( \text{Pre}(\varphi) \), then \( E_\varphi(\sigma) \) is the maximal word (with respect to \( \preceq_{\text{st}} \)) that satisfies \( \varphi \) and
is safe to output. It is maximal because in the definition of store_{\varphi}, \kappa_{\varphi} returns the longest word with lower delays (for lexicographic order), which corresponds to the maximum with respect to \preceq_d. Thus, outputting a greater word (with respect to \preceq_d) would lead to G being empty, meaning that the EM would not be sound. Thus, E_{\varphi} is optimal in Pre(\varphi), since it outputs the maximal word with respect to \preceq_d that allows to be sound and compliant.

4.2. Enforcement Monitors

As in the untimed setting, we define an operational description of an EM whose output is exactly the output of E_{\varphi}, as defined in Definition 16.

Definition 18. An enforcement monitor E for \varphi is a transition system \langle C^E, c^E_0, \Gamma^E, \leadsto_E \rangle s.t.:

- \tl C^E = \text{tw}(\Sigma) \times \Sigma^* \times Q \times \mathbb{R}_{\geq 0} \times \{\top, \bot\}

- \tl c^E_0 = (\epsilon, \epsilon, q_0, 0, \bot) \in C^E is the initial configuration.

- \tl \Gamma^E = (\mathbb{R}_{\geq 0} \times \Sigma) \cup \{\epsilon\} \times Op \times ((\mathbb{R}_{\geq 0} \times \Sigma) \cup \{\epsilon\}) is the alphabet, composed of an optional input, an operation and an optional output.

The set of operations is \{ compute(\cdot), dump(\cdot), pass-uncont(\cdot), store-cont(\cdot), delay(\cdot) \}. Whenever \( (\sigma, \varphi, \sigma') \in \Gamma^E \), it will be noted \sigma / \varphi / \sigma'.

- \tl \leadsto_E is the transition relation defined as the smallest relation obtained by applying the following rules given by their priority order:

  - Compute: \( \langle \epsilon, \sigma_c, q, t, \bot \rangle \xrightarrow{\text{compute}}(\epsilon)_{E} \langle \sigma'_c, \sigma_c, q, t, \top \rangle \), if G(q, \sigma_c) \neq \emptyset, with \sigma'_c = \kappa_{\varphi}(q, \sigma_c) + t, and \sigma_c = \Pi_{\Sigma}(\sigma'_c^{-1}, \sigma_c).

  - Dump: \( \langle (t,b,a).\sigma_b, \sigma_c, q, t_b, \top \rangle \xrightarrow{\text{dump}}(\epsilon)_{E} \langle \sigma_b, \sigma_c, q', t_b, \top \rangle \), with \( q' = q \) after \( (0, a) \).

  - Pass-uncont: \( \langle \sigma_b, \sigma_c, q, t, b \rangle \xrightarrow{(t,a)/\text{pass-uncont}}(\epsilon)_{E} \langle \epsilon, \Pi_{\Sigma}(\sigma_b), \sigma_c, q', t, \bot \rangle \), with \( q' = q \) after \( (0, a) \).

  - Store-cont: \( \langle \sigma_b, \sigma_c, q, t, b \rangle \xrightarrow{(t,c)/\text{store-cont}}(\epsilon)_{E} \langle \epsilon, \Pi_{\Sigma}(\sigma_b), \sigma_c, c, q, t, \bot \rangle \).

  - Delay: \( \langle \sigma_b, \sigma_c, (l, v), t \rangle \xrightarrow{\text{delay}}(\epsilon)_{E} \langle \sigma_b, \sigma_c, (l, v + \delta), t + \delta, b \rangle \).

In a configuration \( (\sigma_b, \sigma_c, q, t, b) \), \sigma_b is the word to be output as time elapses; \sigma_c is the sequence of controllable actions from the input that are not used in \sigma_b and have not been output yet; \( q \) is the state of the semantics reached after reading what has already been output; \( t \) is the current time instant, i.e., the time elapsed since the beginning of the run; and \( b \) indicates whether \sigma_b and \sigma_c should be computed (due to the reception of a new event for example).

The timed word \sigma_b corresponds to nobs(\sigma_b, t) from the definition of store_{\varphi}, whereas \sigma_c is the same as in the definition of store_{\varphi}. The state \( q \) represents \sigma_s, s.t. \( q = \text{Reach}(\sigma_s, t) \).

Proposition 10. The output of E for input \sigma is E_{\varphi}(\sigma).

As in the untimed setting, in Proposition 10, the output of the enforcement monitor is the concatenation of the outputs of the word labelling the path followed by the enforcement monitor when reading \sigma. A formal definition is given in the proof of this proposition, in appendix A.2.

Sketch of proof. The proof is done by induction on \sigma. When receiving a new event, the rule store-cont() can be applied if it is controllable, or rule pass-uncont() if it is uncontrollable. Doing so, the last member of the configuration is set to \bot, meaning that the word to be emitted
The sets of events are: \( \{\text{sync}\} \) and \( \{\text{Write}\} \). Each time the lock is taken and released, we must also wait before issuing a new event. When a Write event is received, we are able to send the controllable event \( \text{Write} \). Once the write is completed, the uncontrollable event \( \text{Auth} \) is sent by the device to authorise writings. Once the \( \text{Auth} \) event is received, we can get the status of a lock through the uncontrollable events \( \text{LockOn} \) and \( \text{LockOff} \). When date \( \text{date} \) is reached, what has been emitted since the last rule was computed by rule compute(). Considering the definition of store, it follows that the output of \( \mathcal{E} \) with input \( \sigma \) at date \( t \) is \( E_\mathcal{E}(\sigma, t) \).

### 4.3. Example

Consider Fig. 3, representing a property modelling the use of some shared writable device. We can get the status of a lock through the uncontrollable events \( \text{LockOn} \) and \( \text{LockOff} \) indicating that the lock has been locked by someone else, and that it is unlocked, respectively. The uncontrollable event \( \text{Auth} \) is sent by the device to authorise writings. Once the \( \text{Auth} \) event is received, we are able to send the controllable event \( \text{Write} \) after having waited some time for synchronisation. Each time the lock is taken and released, we must also wait before issuing a new \( \text{Write} \) order. The sets of events are: \( \Sigma_c = \{\text{Write}\} \) and \( \Sigma_u = \{\text{Auth}, \text{LockOff}, \text{LockOn}\} \).

![Figure 7: Example of Property without uncontrollable events](image)

Figure 7: Example of Property without uncontrollable events

and \( (l_2, \nu) \in S(\epsilon) \), since all uncontrollable words from \( l_1 \) and \( l_2 \) lead to \( l_1 \) or \( l_2 \), which are both accepting states.

We can also follow the execution of an enforcement monitor enforcing the property in Fig. 3,
watching the evolution of the configurations as semantic rules are applied. In a configuration, the input is on the right, the output on the left, and the middle is the current configuration of the enforcement monitor. The variable $t$ defines the global time of the execution. Fig. 8 shows the execution of the enforcement monitor with input $(1, \text{Auth}) \cdot (2, \text{LockOn}) \cdot (4, \text{Write}) \cdot (5, \text{LockOff}) \cdot (6, \text{LockOn}) \cdot (7, \text{Write}) \cdot (8, \text{LockOff})$. In Fig. 8, valuations are represented as integers, giving the value of the only clock $x$ of the property, $\text{LockOff}$ is abbreviated as $\text{off}$, $\text{LockOn}$ as $\text{on}$, and $\text{Write}$ as $\text{w}$. First column depicts the dates of events, then red text is the current output ($\sigma_s$) of the EM, blue text shows the evolution of $\sigma_b$ and green text depicts the remaining input word at this date. We can observe that the final output is the same as the one of the enforcement function: $(1, \text{Auth}) \cdot (2, \text{on}) \cdot (5, \text{off}) \cdot (6, \text{on}) \cdot (8, \text{off}) \cdot (10, \text{w}) \cdot (10, \text{w})$.

**Remark 5.** The EM in Definition 16 output longer timed words than the approach in (Pinisetty et al., 2012) and (Pinisetty et al., 2014c) when applied only with controllable events thanks to optimality considerations. Consider the property in Fig. 7 over the set of controllable actions $\Sigma \supseteq \{\text{Write}\}$, and the input timed word $(1, \text{Write}) \cdot (1.5, \text{Write})$ input to the EM. The output obtained with our approach at date $t = 4$ is $(4, \text{Write}) \cdot (4, \text{Write})$ whereas the output obtained in (Pinisetty et al., 2012) would be $(2, \text{Write})$.

## 5. Related Work

Runtime enforcement was pioneered by the work of Schneider with security automata (Schneider, 2000), a runtime mechanism for enforcing safety properties. In (Schneider, 2000), monitors are able to stop the execution of the system once a deviation of the property has been detected. Later, Ligatti et al. proposed edit-automata, a more powerful model of enforcement monitors able to insert and suppress events from the execution. Later, more general models were proposed where the monitors can be synthesised from regular properties (Falcone et al., 2011). More recently, Bloem et al. (Bloem et al., 2015) presented a framework to synthesise enforcement monitors for reactive systems, called *shields*, from a set of safety properties. A shield acts instantaneously and cannot buffer actions. Whenever a property violation is unavoidable, the shield allows to deviate from the property for $k$ consecutive steps (as in (Charafeddine et al., 2015)). Whenever a second violation occurs within $k$ steps, then the shield enters into a *fail-safe* mode, where it ensures only correctness. Another recent approach by Dolzhenko et al. (Dolzhenko et al., 2015) introduces Mandatory Result Automata (MRAs). MRAs extend edit-automata by refining the input/output relationship of an EM and thus allowing a more precise description of the enforcement abilities of an EM in concrete application scenarios. All the previously mentioned approaches considered untimed specifications, and do not consider uncontrollable events.

In the timed setting, several monitoring tools exist. RT-Mac (Sammapun et al., 2005) permits to verify at runtime timeliness and reliability correctness. LARVA (Colombo et al., 2009a; Colombo et al., 2009b) takes as input safety properties expressed with DATEs (Dynamic Automata with Events and Timers), a timed model similar to timed automata.

In previous work, we introduced *runtime enforcement for timed properties* (Pinisetty et al., 2012) specified by timed automata (Alur and Dill, 1992). We proposed a model of EMs that work as *delayers*, that is, mechanisms that are able to delay the input sequence of timed events to correct it. While (Pinisetty et al., 2012) proposed synthesis techniques only for safety and co-safety properties, we then generalised the framework to synthesise an enforcement monitor for
\begin{verbatim}
t = 0  \epsilon/(\epsilon, (l_0, 0), 0, \bot)/(1, Auth).(2, on).(4, w).(5, off).(6, on).(7, w).(8, off)
down delay(1)
t = 1  \epsilon/(\epsilon, (l_0, 1), 1, \bot)/(1, Auth).(2, on).(4, w).(5, off).(6, on).(7, w).(8, off)
down pass-uncont((1, Auth))
t = 1  (1, Auth)/(\epsilon, \epsilon, (l_1, 1), 1, \top)/(2, on).(4, w).(5, off).(6, on).(7, w).(8, off)
down compute()
t = 1  (1, Auth)/(\epsilon, \epsilon, (l_1, 1), 1, \top)/(2, on).(4, w).(5, off).(6, on).(7, w).(8, off)
down delay(1)
t = 2  (1, Auth)/(\epsilon, \epsilon, (l_2, 2), 2, \bot)/(2, on).(4, w).(5, off).(6, on).(7, w).(8, off)
down pass-uncont((2, on))
t = 2  (1, Auth).(2, on)/(\epsilon, \epsilon, (l_2, 2), 2, \bot)/(2, on).(4, w).(5, off).(6, on).(7, w).(8, off)
down compute()
t = 4  (1, Auth).(2, on)/(\epsilon, \epsilon, (l_4, 4), 4, \bot)/(4, w).(5, off).(6, on).(7, w).(8, off)
down store-cont((4, w))
t = 4  (1, Auth).(2, on)/(\epsilon, \epsilon, (l_4, 4), 4, \bot)/(5, off).(6, on).(7, w).(8, off)
down delay(1)
t = 5  (1, Auth).(2, on)/(\epsilon, \epsilon, (l_5, 5), 5, \bot)/(5, off).(6, on).(7, w).(8, off)
down pass-uncont((5, off))
t = 5  (1, Auth).(2, on).(5, off)/(\epsilon, \epsilon, (l_1, 0), 5, \bot)/(6, on).(7, w).(8, off)
down compute()
t = 6  (1, Auth).(2, on).(5, off)/(\epsilon, \epsilon, (l_1, 1), 6, \bot)/(6, on).(7, w).(8, off)
down pass-uncont((6, on))
t = 6  (1, Auth).(2, on).(5, off).(6, on)/(\epsilon, \epsilon, (l_1, 2), 6, \bot)/(7, w).(8, off)
down compute()
t = 7  (1, Auth).(2, on).(5, off).(6, on)/(\epsilon, \epsilon, (l_2, 2), 7, \bot)/(7, w).(8, off)
down store-cont((7, w))
t = 7  (1, Auth).(2, on).(5, off).(6, on)/(\epsilon, \epsilon, (l_2, 2), 7, \bot)/(8, off)
down compute()
t = 7  (1, Auth).(2, on).(5, off).(6, on)/(\epsilon, \epsilon, (l_2, 2), 7, \bot)/(8, off)
down delay(1)
t = 8  (1, Auth).(2, on).(5, off).(6, on)/(\epsilon, \epsilon, (l_3, 8, \bot))/(8, off)
down pass-uncont((8, off))
t = 8  (1, Auth).(2, on).(5, off).(6, on)/(\epsilon, \epsilon, (l_1, 0), 8, \bot)/(\epsilon)
down compute()
t = 8  (1, Auth).(2, on).(5, off).(6, on)/(\epsilon, \epsilon, (l_1, 0), 8, \bot)/(\epsilon)
down delay(2)
t = 10 (1, Auth).(2, on).(5, off).(6, on)/(\epsilon, \epsilon, (l_1, 2), 10, \bot)/(\epsilon)
down dump((10, w))
t = 10 (1, Auth).(2, on).(5, off).(6, on)/(\epsilon, \epsilon, (l_1, 2), 10, \bot)/(\epsilon)
down dump((10, w))
t = 10 (1, Auth).(2, on).(5, off).(6, on)/(\epsilon, \epsilon, (l_1, 2), 10, \bot)/(\epsilon)
\end{verbatim}

Figure 8: Execution of an enforcement monitor with input \((1, Auth)\). \((2, LockOn)\). \((4, Write)\). \((5, LockOff)\). \((6, LockOn)\). \((7, Write)\). \((8, LockOff)\)
any regular timed property (Pinisetty et al., 2014b; Pinisetty et al., 2014c). In (Pinisetty et al., 2014a), we considered parametric timed properties, that is timed properties with data-events containing information from the execution of the monitored system. In our approach, the optimality of the enforcement mechanism is based on the maximisation of the length of the output sequence. When applied in the case of controllable events only, this improves the preceding results.

Basin et al. (Basin et al., 2011) introduced uncontrollable events for security automata (Schneider, 2000). The approach in (Basin et al., 2011) allows to enforce safety properties where some of the events in the specification are uncontrollable. More recently, they proposed a more general approach (Basin et al., 2013) related to enforcement of security policies with controllable and uncontrollable events. They presented several complexity results and how to synthesise EMs. In case of violation of the property, the system stops the execution. They handle discrete time, and clock ticks are considered as uncontrollable events. In our approach, we consider dense time using the expressiveness of timed automata, any regular properties, and our monitor are more flexible since they block the system only when delaying events cannot prevent from violating the property, thus offering the possibility to correct many violations.

6. Conclusion and Future Work

This paper extends previous work on enforcement monitoring with uncontrollable events, which are only observable by an EM. We present a framework for both untimed and timed regular properties, described with (untimed) automata and timed automata, respectively. We provide a functional and an operational description of the enforcement mechanism, and show their equivalence. Adding uncontrollable events leads to the necessity of changing the order between controllable and uncontrollable events, which requires some existing notions to be adapted. Therefore, we replace transparency with compliance, and then give EMs, i.e. enforcement functions and enforcement monitors, for regular properties and regular timed properties. Since not every property can be enforced, we also give a condition, depending on the property and the input word, indicating whether the EM is sound with respect to the property under scrutiny or not. The EMs output immediately all the uncontrollable events received, and store the controllable ones, until soundness can be guaranteed. Then, they output events only when they can ensure that soundness will be satisfied. The proposed EMs are then sound and compliant, even with reception of some uncontrollable events. They are also optimal in the sense that they output the longest possible word, with the least possible dates in the timed setting.

One possible extension is to take some risks, outputting events even if some uncontrollable events could lead to a bad state, and introducing for example some probabilities. Implementing the given enforcement devices for the untimed setting is pretty straightforward, whereas implementation in the timed setting needs more attention due to computing in timed models. Another interesting direction for further investigation is to use game theory in order to compute the behaviour of the EM. This approach should permit to compute the behaviour before the execution, thus leading to an optimised implementation.
Optimal Enforcement of (Timed) Properties with Uncontrollable Events

References


Appendix A. Proofs

A.1. Proofs for the Untimed Setting

In all this section, we will use the notations from Section 3, meaning that $\varphi$ is a property whose associated automaton is $A_{\varphi} = (Q, q_0, \Sigma, \rightarrow, F)$. In some proofs, we also use notations from Definition 8.

**Proposition 1.** $E_{\varphi}$ as defined in Definition 8 is an enforcement function.

**Proof.** Let us consider $\sigma \in \Sigma^*$, and $\sigma' \in \Sigma^*$. If $\sigma' = \varepsilon$, then $E_{\varphi}(\sigma) = E_{\varphi}(\sigma, \varepsilon) \leq E_{\varphi}(\sigma, \sigma')$. Otherwise, let us consider $(\sigma_s, \sigma_0) = store_{\varphi}(\sigma), a = \sigma'(1)$, and $(\sigma_i, \sigma_a) = store_{\varphi}(\sigma, a)$. Then, if $a \in \Sigma_m$, $\sigma_i = \sigma_s.a.\sigma'_s$, where $\sigma_s'$ is defined in Definition 8, meaning that $\sigma_s \leq \sigma_i$. If $a \in \Sigma_v$, then $\sigma_i = \sigma_s.a.\sigma'_s$, where $\sigma'_s$ is defined in Definition 8, thus again, $\sigma_s \leq \sigma_i$. In both cases, $E_{\varphi}(\sigma) = \sigma_s \leq \sigma_i = E_{\varphi}(\sigma, a)$. Since the order $\leq$ is transitive, this means that $E_{\varphi}(\sigma) \leq E_{\varphi}(\sigma, a) \leq E_{\varphi}(\sigma, a, \sigma'(2)) \leq \ldots \leq E_{\varphi}(\sigma, \sigma')$. Thus $E_{\varphi}$ is an enforcement function. □

**Lemma 1.** $\forall \sigma \in \Sigma^*_v, \forall a \in \Sigma_v, I(\sigma) \subseteq I(\sigma, a)$.

**Proof.** For $\sigma \in \Sigma^*_v$, let $P(\sigma)$ be the predicate “$\forall a \in \Sigma_v, I(\sigma) \subseteq I(\sigma, a)$”. Let us show by induction that $P(\sigma)$ holds for every $\sigma \in \Sigma^*_v$.

--- Induction basis: if $a \in \Sigma_v$, then since $I(\varepsilon) = \emptyset$, $I(\varepsilon) \subseteq I(a)$. Thus, $P(\varepsilon)$ holds.

--- Induction step: let us suppose that for $\sigma \in \Sigma^*_v$, $|\sigma| \leq n$, $P(\sigma)$ holds. Let us then consider $\sigma' \in \Sigma^*_v$, $|\sigma'| = n + 1$, and $a \in \Sigma_v$. Let $h, \sigma_0 \in \Sigma_v \times \Sigma^*_v$ be s.t. $\sigma = h.\sigma_0$ (they must exist since $|\sigma| > 0$). Then, $|\sigma_0| = n$, and by induction hypothesis, $P(\sigma_0)$ holds, meaning that $I(\sigma_0) \subseteq I(\sigma_0, a)$. Moreover, following the definition of $S(\sigma_0, a), S(\sigma_0) \subseteq S(\sigma_0, a)$. It follows that $S(\sigma_0) \cup I(\sigma_0) \subseteq S(\sigma_0, a) \cup I(\sigma_0, a)$, and thus $I(\sigma) = I(h.\sigma_0) = \textrm{Pred}_h(S(\sigma_0) \cup I(\sigma_0)) \subseteq \textrm{Pred}_h(S(\sigma_0, a) \cup I(\sigma_0, a)) = I(h.\sigma_0, a) = I(\sigma, a)$. This means that $P(\sigma, a)$ holds.

Thus, by induction on the size of $\sigma \in \Sigma^*_v$, for all $\sigma \in \Sigma^*_v$, $P(\sigma)$ holds. This means that for all $\sigma \in \Sigma^*_v$, for all $a \in \Sigma_v, I(\sigma) \subseteq I(\sigma, a)$. □

**Lemma 2.** $\forall \sigma \in \Sigma^*_v, \forall q \in Q, \forall u \in \Sigma_v, (q \in S(\sigma)) \implies (q \text{ after } u \in S(\sigma) \cup I(\sigma))$.

**Proof.** For $\sigma \in \Sigma^*_v$, let $P(\sigma)$ be the predicate “$\forall q \in Q, \forall u \in \Sigma_v, (q \in S(\sigma)) \implies (q \text{ after } u \in S(\sigma) \cup I(\sigma))$”. Let us show by induction that $P(\sigma)$ holds for any $\sigma \in \Sigma_v$.

--- Induction basis: let us consider $u \in \Sigma_v$ and $q \in S(\sigma)$. Then, since $u \in \Sigma_v, u \in \Sigma^*_v$, and following the definition of $S(\sigma)$, $q$ after $u \in S(\sigma), \sigma$. Thus, $q$ after $u \in S(\sigma) \cup I(\sigma)$. □
—Induction step: let us suppose that for $\sigma \in \Sigma^*_s$, $P(\sigma)$ holds. Let us then consider $u \in \Sigma_u$, $a \in \Sigma_a$, and $q \in S(a,a)$. Then, either $q \in S(\sigma)$ or $q \in \text{max}_{\Sigma} \{Y \subseteq F_G \mid Y \cap u\text{Pred}(Y \cup \{\sigma,a\}) = \emptyset\}$. If $q \in S(\sigma)$, then by induction hypothesis, $P(\sigma)$ holds, meaning that $q$ after $u \in S(\sigma) \cup I(\sigma)$. Following lemma 1, $I(\sigma) \subseteq I(\sigma,a)$, and since $S(\sigma) \subseteq S(\sigma,a)$, it follows that $S(\sigma) \cup I(\sigma) \subseteq S(\sigma,a) \cup I(\sigma,a)$. Thus, $q$ after $u \in S(\sigma,a) \cup I(\sigma,a)$. Otherwise, $q \in \text{max}_{\Sigma} \{Y \subseteq F_G \mid Y \cap u\text{Pred}(Y \cup \{\sigma,a\}) = \emptyset\}$, and thus $q$ after $u \in S(\sigma,a) \cup I(\sigma,a)$. Thus, $P(\sigma,a)$ holds.

By induction on $\sigma$, it follows that $P(\sigma)$ holds for any $\sigma \in \Sigma^*_s$. Thus, for all $\sigma \in \Sigma^*_s$, for all $u \in \Sigma_u$, for all $q \in Q$, $(q \in S(\sigma) \cup I(\sigma)) \implies (q \text{ after } u \in S(\sigma) \cup I(\sigma))$. □

Lemma 3. $\forall \sigma \in \Sigma^*_s, \forall q \in S(\sigma) \cup I(\sigma), G(q, \sigma) \neq \emptyset$.

Proof. For $\sigma \in \Sigma^*_s$, let $P(\sigma)$ be the predicate “$\forall q \in S(\sigma) \cup I(\sigma), G(q, \sigma) \neq \emptyset$”. Let us show by induction that $P(\sigma)$ holds for any $\sigma \in \Sigma^*_s$.

—Induction basis: let us consider $q \in S(\epsilon) \cup I(\epsilon)$. Then, since $I(\epsilon) = \emptyset$, $q \in S(\epsilon)$. Following the definition of $S(\epsilon)$, this means that $\epsilon$ is s.t. $\epsilon \ll \epsilon$ and $q$ after $\epsilon = q \in S(\epsilon) = S(\epsilon^{-1})$. Thus, $\epsilon \in G(q, \epsilon)$, meaning that $G(q, \epsilon) \neq \emptyset$, and thus that $P(\epsilon)$ holds.

—Induction step: let us suppose that for $n \in \mathbb{N}$, for all $\sigma \in \Sigma^*_s$ s.t. $|\sigma| \leq n$, $P(\sigma)$ holds. Let us then consider $\sigma \in \Sigma^*_s$ s.t. $|\sigma| = n$, $a \in \Sigma_a$, and $q \in S(\sigma,a) \cup I(\sigma,a)$. Then, we consider two cases:

- $q \in S(\sigma,a)$, then $\epsilon$ is s.t. $\epsilon \ll \sigma.a$ and $q$ after $\epsilon \in S(\sigma,a) = S(\epsilon^{-1}.(\sigma.a))$, thus $\epsilon \in G(q, \sigma.a)$.

- $q \in I(\sigma,a)$, then let $(h, \sigma_0) \in \Sigma \times \Sigma^{\omega}$ be s.t. $h.\sigma_0 = \sigma.a$ (they must exist since $|\sigma.a| > 0$). Then, $I(\sigma.a) = I(h, \sigma_0) = \text{Pred}_h(S(\sigma),I(\sigma_0))$, meaning that $q \in \text{Pred}_h(S(\sigma),I(\sigma_0))$. By induction hypothesis, since $|\sigma_0| = |\sigma| = n$, $P(\sigma_0)$ holds, meaning that $G(q \text{ after } h, \sigma_0) \neq \emptyset$. Let us then consider $w \in G(q \text{ after } h, \sigma_0)$. Then, $w$ is s.t. $w \ll \sigma_0$ and $(q \text{ after } h) \in w \in S(w^{-1}.\sigma_0)$. Thus, $(h.w \ll w \sigma_0$, and $q$ after $(h.w) \in S((h.w)^{-1}.(h.\sigma_0))$. Thus, $h.w \in G(q, h.\sigma_0) = G(q, \sigma.a)$.

In both cases, $G(q, \sigma.a) \neq \emptyset$, meaning that $P(\sigma.a)$ holds. By induction on the size of $\sigma \in \Sigma^*_s$, it follows that $P(\sigma)$ holds for any $\sigma \in \Sigma^*_s$, for all $q \in S(\sigma) \cup I(\sigma)$, $G(q, \sigma) \neq \emptyset$. □

Lemma 4. $\forall \sigma \in \Sigma^*, (\sigma \notin \text{Pre}(\varphi) \land (s_\varphi, s_\psi) = \text{store}_{\varphi}(\sigma)) \implies (s_\varphi = s_{\varphi}}_{\psi} \land s_\psi = s_{\psi}}_{\varphi})$.

Proof. For $\sigma \in \Sigma^*$, let $P(\sigma)$ be the predicate “$(\sigma \notin \text{Pre}(\varphi) \land (s_\varphi, s_\psi) = \text{store}_{\varphi}(\sigma)) \implies (s_\varphi = s_{\varphi}}_{\psi} \land s_\psi = s_{\psi}}_{\varphi})$. Let us show by induction that $P(\sigma)$ holds for any $\sigma \in \Sigma^*$.

—Induction basis: $(\text{store}_{\varphi}(\sigma) = (\epsilon, \epsilon)$, and since $\epsilon}_{\varphi} = \epsilon_{\psi} = \epsilon$, $P(\epsilon)$ holds.

—Induction step: let us suppose that for $\sigma$ s.t. $\sigma \in \Sigma^*_s$, $P(\sigma)$ holds. Let us then consider $a \in \Sigma_a$, $(s_\varphi, s_\psi) = \text{store}_{\varphi}(a)$. Then, if $s_\varphi \in \text{Pre}(\varphi)$, $P(\sigma.a)$ holds. Let us now consider that $s_\varphi \notin \text{Pre}(\varphi)$. Then, since $\text{Pre}(\varphi)$ is extension-closed, $\varphi \notin \text{Pre}(\varphi)$, and thus by induction hypothesis, $s_\varphi = s_{\varphi}}_{\psi}$. We consider two cases:

- $a \in \Sigma_a$, then $s_\varphi = s_{\varphi}}_{\varphi}$, with $s_{\varphi}}_{\varphi} \in G(\text{Reach}(s_\varphi,a), \sigma.e) \cup \{\epsilon\}$. Since $s_\varphi \notin \text{Pre}(\varphi)$, $G(\text{Reach}(s_\varphi,a)) = s_{\varphi}}_{\varphi} \in \emptyset$.

- $a \in \Sigma_a$, then $s_\varphi = s_{\varphi}}_{\varphi}$, with $s_{\varphi}}_{\varphi} \in G(s_{\varphi}, \sigma.e) \cup \{\epsilon\}$. Since $s_\varphi \notin \text{Pre}(\varphi), G(\text{Reach}(s_\varphi,a)) = s_{\varphi}}_{\varphi} \in \emptyset$. Moreover, since $s_\varphi \notin \text{Pre}(\varphi), G(\text{Reach}(s_\varphi,a)) = s_{\varphi}}_{\varphi} \in \emptyset$. It follows that $s_{\varphi}}_{\varphi} \in \epsilon$, meaning that $s_\varphi = s_{\varphi}}_{\psi} = s_{\varphi}}_{\varphi} \in \emptyset$, and $s_{\varphi}}_{\varphi} = s_{\varphi}}_{\varphi} \in \emptyset$. Moreover, since $s_\varphi \notin \text{Pre}(\varphi), G(\text{Reach}(s_\varphi,a)) = s_{\varphi}}_{\varphi} \in \emptyset$. Thus, $G(\text{Reach}(s_\varphi,a), \sigma.a) = \emptyset$. It follows that $s_{\varphi}}_{\varphi} \in \epsilon$, meaning that $s_\varphi = s_{\varphi}}_{\psi} = s_{\varphi}}_{\psi} \in \emptyset$, and $s_{\varphi}}_{\varphi} = s_{\varphi}}_{\varphi} \in \emptyset$.

In both cases, $P(\sigma.a)$ holds. By induction on $\sigma \in \Sigma^*$, for all $\sigma \in \Sigma^*$, if $\sigma \notin \text{Pre}(\varphi)$ and $(s_\varphi, s_\psi) = \text{store}_{\varphi}(\sigma)$, then $s_\varphi = s_{\varphi}}_{\psi}$ and $s_\psi = s_{\varphi}}_{\varphi}$. □
Proposition 2. $E_\phi$ is sound with respect to $\phi$ in $\text{Pre}(\phi)$, as per Definition 3.

Proof. Let $P(\sigma)$ be the predicate: “($\sigma \in \text{Pre}(\phi) \wedge (\sigma_s, \sigma_c) = \text{store}_\phi(\sigma)$) $\implies$ ($E_\phi(\sigma) \models \phi \wedge \text{Reach}(\sigma_s) \in S(\sigma_c)$)”. Let us prove by induction that for any $\sigma \in \Sigma^*$, $P(\sigma)$ holds.

--- Induction basis: if $\epsilon \in \text{Pre}(\phi)$, then following the definition of $\text{Pre}(\phi)$, $G(\text{Reach}(\epsilon), \epsilon) \neq \emptyset$. Thus $\epsilon \in G(\text{Reach}(\epsilon), \epsilon)$ (since $\epsilon$ is the only word satisfying $\epsilon \leq \epsilon$). This means that $\text{Reach}(\epsilon)$ after $\epsilon$ = $\text{Reach}(\epsilon)$ in $S(\epsilon)$. Considering that $\text{store}_\phi(\epsilon) = (\epsilon, \epsilon)$, it follows that $E_\phi(\epsilon) = \epsilon$, and thus, since $S(\epsilon) \subseteq F_G$, $E_\phi(\epsilon) \models \phi$. Thus $P(\epsilon)$ holds.

--- Induction step: Suppose now that, for $\sigma \in \Sigma^*$, $P(\sigma)$ holds. Let us consider $a \in \Sigma_c, (\sigma_s, \sigma_c) = \text{store}_\phi(\sigma)$, and $(\sigma_1, \sigma_2) = \text{store}_\phi(\sigma_a)$. Let us prove that $P(\sigma_a)$ holds. We consider three different cases:

1. $(\sigma, a) \notin \text{Pre}(\phi)$. Then $P(\sigma_a)$ holds.
2. $(\sigma, a) \in \text{Pre}(\phi)$ and $\sigma \notin \text{Pre}(\phi)$, then, since $\text{Pre}(\phi)$ is extension-closed, it follows that $\sigma \wedge a \in \{w \in \Sigma^* \mid G(\text{Reach}(w), w) \neq \emptyset\}$, meaning that $G(\text{Reach}(\sigma \wedge a), \sigma \wedge a) \neq \emptyset$. Moreover, since $\sigma \notin \text{Pre}(\phi)$, following lemma 4, $\sigma_s = \sigma_{\Sigma_s}$ and $\sigma_c = \sigma_{\Sigma_c}$. Now, we consider two cases:

   - If $a \in \Sigma_n$, then $(\sigma, a) = (\sigma_{\Sigma_n}, a) = (\sigma, a)$, and $(\sigma, a)_{\Sigma_n} = (\sigma_{\Sigma_n}, a) = \sigma_{\Sigma_n}$. Thus, $G(\text{Reach}(\sigma \wedge a), \sigma_{\Sigma_n}) \neq \emptyset$, meaning that $\sigma' = (\sigma \wedge a)^{-1} \sigma \in G(\text{Reach}(\sigma \wedge a), \sigma_{\Sigma_n})$. Thus, following the definition of $G$, $\text{Reach}(\sigma \wedge a)$ after $\sigma' = \text{Reach}(\sigma \wedge a, \sigma') = \text{Reach}(\sigma) \in S(\sigma_{\Sigma_n}^{-1}, \sigma') = S(\sigma_{\Sigma_n})$. Moreover, since $S(\sigma_{\Sigma_n}) \subseteq F_G$, $E_\phi(\sigma_a) = \sigma \models \phi$. This means that $P(\sigma_a)$ holds.

   - If $a \in \Sigma_c$, then $(\sigma, a)_{\Sigma_c} = \sigma_{\Sigma_c} = \sigma$ and $(\sigma, a)_{\Sigma_c} = \sigma_{\Sigma_c} = \sigma_{\Sigma_c}$. Thus, $G(\text{Reach}(\sigma \wedge a), \sigma_{\Sigma_c}) \neq \emptyset$, meaning that $\sigma' = (\sigma \wedge a)^{-1} \sigma \in G(\text{Reach}(\sigma \wedge a), \sigma_{\Sigma_c})$. In the case where $a \notin \Sigma_n$, it follows that $\text{Reach}(\sigma) \in S(\sigma_{\Sigma_n})$ and thus $E_\phi(\sigma_a) \models \phi$. This means that $P(\sigma_a)$ holds.

Thus, if $\sigma \in \text{Pre}(\phi)$ but $\sigma \notin \text{Pre}(\phi)$, $P(\sigma_a)$ holds.

3. $\sigma \in \text{Pre}(\phi)$ (and then $(\sigma, a) \in \text{Pre}(\phi)$ since $\text{Pre}(\phi)$ is extension-closed). Then, by induction hypothesis, $P(\sigma)$ holds, meaning that $\text{Reach}(\sigma_s) \in S(\sigma_c)$ and $E_{\phi}(\sigma) \models \phi$. Again, we consider two cases:

   - If $a \in \Sigma_n$, then, since $\text{Reach}(\sigma_s) \in S(\sigma_c)$, following lemma 2, $\text{Reach}(\sigma_s) \wedge a = \text{Reach}(\sigma_s, a) \in S(\sigma_s) \cup I(\sigma_c)$. Following lemma 3, $G(\text{Reach}(\sigma_s, a), \sigma_{\Sigma_n}) \neq \emptyset$. Thus, $\sigma' = (\sigma \wedge a)^{-1} \sigma \in G(\text{Reach}(\sigma_s, a), \sigma_{\Sigma_n})$. It follows that $\text{Reach}(\sigma_s, a, \sigma') = \text{Reach}(\sigma_s) \in S(\sigma_{\Sigma_n}^{-1}, \sigma') = S(\sigma_{\Sigma_n})$, and thus, since $S(\sigma_{\Sigma_n}) \subseteq F_G$, $E_{\phi}(\sigma_a) = \sigma \models \phi$. Henceforth, $P(\sigma_a)$ holds.

   - If $a \in \Sigma_c$, then, since $\text{Reach}(\sigma_s) \in S(\sigma_c)$ and $S(\sigma_{\Sigma_n}) \subseteq S(\sigma_{\Sigma_c}), \text{Reach}(\sigma_s) \in S(\sigma_{\Sigma_c})$. Following lemma 3, $G(\text{Reach}(\sigma_s), \sigma_{\Sigma_c}) \neq \emptyset$. Thus, $\sigma' = (\sigma \wedge a)^{-1} \sigma \in G(\text{Reach}(\sigma_s), \sigma_{\Sigma_c})$. In the case where $a \notin \Sigma_n$, this leads to $\sigma \models S(\sigma_{\Sigma_n})$ and $E_{\phi}(\sigma_a) \models \phi$. Henceforth, $P(\sigma_a)$ holds.

Thus, if $\sigma \in \text{Pre}(\phi)$, $P(\sigma_a)$ holds.

In all cases, $P(\sigma_a)$ holds. Thus, $P(\sigma) \implies P(\sigma_a)$. By induction on $\sigma$, $\forall \sigma \in \Sigma^*, (\sigma \in \text{Pre}(\phi) \wedge (\sigma_s, \sigma_c) = \text{store}_\phi(\sigma)) \implies (E_{\phi}(\sigma) \models \phi \wedge \text{Reach}(\sigma_s) \in S(\sigma_c))$. In particular, for all $\sigma \in \Sigma^*$, $(\sigma \in \text{Pre}(\phi)) \implies (E_{\phi}(\sigma) \models \phi)$. This means that $E_{\phi}$ is sound with respect to $\phi$ in $\text{Pre}(\phi)$.

\square

Proposition 3. $E_\phi$ is compliant, as per Definition 4.

Proof. For $\sigma \in \Sigma^*$, let $P(\sigma)$ be the predicate: “($\sigma_s, \sigma_c = \text{store}_\phi(\sigma)$) $\implies$ (store$_\phi(\sigma) \models \phi \wedge \text{Reach}(\sigma_s) \in S(\sigma_c)$)”. Let us prove that for all $\sigma \in \Sigma^*, P(\sigma)$ holds.

--- Induction basis: $\text{store}_\phi(\epsilon) = (\epsilon, \epsilon)$, and $\epsilon_{\Sigma_s} = \epsilon_{\Sigma_c} = \epsilon_{\Sigma_a}$. Thus $P(\epsilon)$ holds.

--- Induction step: Let us suppose that for $\sigma \in \Sigma^*$, $P(\sigma)$ holds. Let us consider $(\sigma_s, \sigma_c) = \text{store}_\phi(\sigma)$, $a \in \Sigma$, and $(\sigma_1, \sigma_2) = \text{store}_\phi(\sigma_a)$. Let us prove that $P(\sigma_a)$ holds.

--- Case 1: $a \in \Sigma_n$. Then, $\sigma_a = \sigma_s \sigma_a \sigma'_a$, where $\sigma'_a$ is defined in Definition 8, and $\sigma_1 \sigma_2 = \sigma_a \sigma_a \sigma_c$. Therefore, $\sigma_1 \sigma_2 = (\sigma_1 \sigma_2)_{\Sigma_a} \sigma_c$, since $\sigma_d \in \Sigma^*$. Thus, $\sigma_1 \sigma_2 \sigma_a = \sigma_1 \sigma_2 \sigma_a \sigma_c$. Since $P(\sigma)$ holds, $\sigma_1 \sigma_2 \sigma_a \sigma_c = \sigma_{\Sigma_c} = (\sigma_1 \sigma_2)_{\Sigma_a}$. Thus, $P(\sigma_a)$ holds. \square
Moreover, since $\sigma'_{a} \in \Sigma_{e}^{*}$, $\sigma(x_{sa}) = \sigma_{a}x_{sa}$. Since $P(\sigma)$ holds, this means that $\sigma(x_{sa}) = \sigma_{a}x_{sa} = (\sigma.a)_{x_{sa}}$.

Thus $P(\sigma.a)$ holds.

Case 2: $a \in \Sigma_{c}$. Then $\sigma_{t} = \sigma_{a}x_{sa}'$, where $x_{sa}'$ is defined in Definition 8, and $\sigma_{t}x_{sa} = \sigma_{a}x_{sa}$.

Therefore, $\sigma(\Sigma_{e}, x_{sa}) = (\sigma_{t}x_{sa})_{\Sigma_{c}} = \sigma_{a}x_{sa} = (\sigma.a)_{x_{sa}}$. Since $P(\sigma)$ holds, this means that $\sigma(x_{sa}) = \sigma_{a}x_{sa} = (\sigma.a)_{x_{sa}}$.

Moreover, since $\sigma'_{a} \in \Sigma_{c}$, $\sigma(x_{sa}) = \sigma_{a}x_{sa}$. Since $P(\sigma)$ holds, this means that $\sigma(x_{sa}) = \sigma_{a}x_{sa} = (\sigma.a)_{x_{sa}}$.

Thus $P(\sigma.a)$ holds.

In both cases, $P(\sigma.a)$ holds. Thus, for all $\sigma \in \Sigma^{*}$, for all $a \in \Sigma$, $P(\sigma) \implies P(\sigma.a)$.

By induction on $\sigma$, for all $\sigma \in \Sigma^{*}$, $(\sigma.s, \sigma.e) = \text{store}_{\varphi}(\sigma) \implies (\sigma_{t}x_{sa})_{\Sigma_{c}} = \sigma_{a}x_{sa} = (\sigma.a)_{x_{sa}}$.

Moreover, if $\sigma \in \Sigma^{*}$, $u \in \Sigma_{u}$, $(\sigma_{a}, \sigma_{e}) = \text{store}_{\varphi}(\sigma)$, and $(\sigma_{t}, \sigma_{u}) = \text{store}_{\varphi}(\sigma.u)$, then $\sigma_{t} = \sigma_{a}u.x_{sa}'$, where $x_{sa}'$ is defined in Definition 8. Thus $\sigma_{t}.u \notin \sigma_{a}x_{sa}$, and since $\sigma_{t} = \text{store}_{\varphi}(\sigma)$, and $\sigma_{t} = \text{store}_{\varphi}(\sigma)u$, it follows that $E_{\varphi}(\sigma).u \notin E_{\varphi}(\sigma.u)$. Thus, for all $\sigma \in \Sigma^{*}$, $E_{\varphi}(\sigma) \notin \sigma_{a}x_{sa} = (\sigma.a)_{x_{sa}} \in \Sigma_{c}$. Thus $P(\sigma.a)$ is compliant.

Lemma 5. $\forall \sigma \in \Sigma^{*}, \forall q \in \Sigma_{q}$ (q $\notin S(\sigma)$) $\implies (\exists \sigma_{1} \in \Sigma_{q}, q \text{ after } \sigma_{1} \in F \land \forall \sigma'_{a} \in \sigma_{1} \land \forall q' \in \sigma_{a} \land \forall q' \in \sigma_{a} \implies q \text{ after } \sigma'_{a} \notin S(\sigma) \cup I(\sigma))$.

Proof. For $\sigma \in \Sigma_{q}$ and $q \in \Sigma_{q}$, let $P(\sigma, q)$ be the predicate $(q \notin S(\sigma) \land q \text{ after } \sigma_{a} \in F \land \exists \sigma'_{a} \in \sigma_{1} \land \forall q' \in \sigma_{a} \land \forall q' \in \sigma_{a} \implies q \text{ after } \sigma'_{a} \notin S(\sigma) \cup I(\sigma))$. Let us show the contrapositive of the lemma, that is, for all $\sigma \in \Sigma_{q}$ and $q \in \Sigma_{q}$, $P(\sigma, q)$ $\implies q \in S(\sigma)$. We consider two cases:

If $\sigma = \epsilon$, let us consider $q \in \Sigma_{q}$ s.t. $P(\epsilon, q)$ holds. Then, since $\epsilon \in \Sigma_{q}$ and there does not exist a word $w$ satisfying $w \in \Sigma_{q} \land \wedge w \neq \epsilon$, it follows that $\epsilon \notin F$. Let us consider $\sigma_{1} \in \Sigma_{q}$.

Then, since $P(\epsilon, q)$ holds, either $q$ after $\sigma_{a} \in F$, or there exists $\sigma_{l} \in \Sigma_{q}$ such that $\sigma_{l} \neq \epsilon$ and $q$ after $\sigma_{l} \in S(\epsilon) \cup I(\epsilon)$. In this last case, since $I(\epsilon) = \emptyset$, $q$ after $\sigma_{l} \in S(\epsilon)$. Following the definition of $S(\epsilon)$, since $\sigma_{l} \in \Sigma_{q}$, $(q \text{ after } \sigma_{l}) \in (\sigma_{l} \neq \epsilon \implies q \text{ after } \sigma_{l} \in F)$. Thus, in all cases $q \text{ after } \sigma_{a} \in F$. Thus, for all $\sigma \in \Sigma_{q}$, $q$ after $\sigma_{a} \in F$, meaning that $q \in S(\sigma)$.

If $\sigma \neq \epsilon$, there exists $\sigma_{e} \in \Sigma_{e}$ and $a \in \Sigma$ s.t. $\sigma = \sigma_{e}.a$, meaning that $S(\sigma)$ is s.t. $S(\sigma) = S(\sigma') \cup \max_{e}(\{Z \subseteq F \mid Z \cap \cup \text{Pred}(Z \cup I(\sigma)) = \emptyset\})$. Let us consider $q \in \Sigma_{q}$ s.t. $P(\sigma, q)$ holds. Then, we define $Y = \{q \text{ after } \sigma_{a} \in \Sigma_{q} \land \forall q' \in \sigma_{a} \land \forall q' \in \sigma_{a} \implies q \text{ after } \sigma'_{a} \notin S(\sigma) \cup I(\sigma)\}$. Since $P(\sigma, q)$ holds, $Y \subseteq F$. Moreover, if $y \in Y$ and $u \in \Sigma_{u}$, then:

- either $y$ after $u \in S(\sigma) \cup I(\sigma)$, and then $y$ after $u \in (Y \cup S(\sigma) \cup I(\sigma))$,

or $y$ after $u \notin S(\sigma) \cup I(\sigma)$. Then, if $\sigma_{u} \in \Sigma_{u}$ is s.t. $y = q$ after $\sigma_{a} \in S(\sigma) \cup I(\sigma)$, then $y$ after $u = (q \text{ after } \sigma_{a} \in S(\sigma) \cup I(\sigma))$. Since $\sigma_{u} \in \Sigma_{u}$, $y$ after $u \in (Y \cup S(\sigma) \cup I(\sigma))$.

Thus, $q \in \Sigma_{q}$, $q \in \Sigma_{q}$, $P(\sigma, q) \implies q \in S(\sigma)$. This means that the contrapositive also holds, thus $q \notin S(\sigma) \implies \neg P(\sigma, q)$, meaning that $q \notin S(\sigma) \implies (\exists \sigma_{a} \in \Sigma_{q}, q \text{ after } \sigma_{a} \in F \land \forall \sigma'_{a} \in \Sigma_{q} \land \forall q' \in \sigma_{a} \land \forall q' \in \sigma_{a} \implies q \text{ after } \sigma'_{a} \notin S(\sigma) \cup I(\sigma))$.
The output of the enforcement monitor

For a word $q$, let us suppose now that for some $c$, $E(q, c)$ follows that $q \notin E$. Let us introduce some notation for this proof: for a word $E$, if $E$ exists number of times (at most until all the controllable events of $s$), then, we can again use lemma 5 to find a word $\sigma$. This means that, if $\sigma_0 = \text{Reach}(\sigma)$, this is not possible, or that $\sigma_0 \notin E(\sigma_0 \cup \{q\})$. Let us consider $q = \text{Reach}(\sigma_0 \cup \{q\})$ and $\sigma_1 = \sigma_0^q \sigma$. Then, $q \notin E(\sigma_1)$. Following lemma 5, this means that there exists $\sigma_0 \in \Sigma^*$ s.t. $q$ after $\sigma_0 \notin E$ and for all $\sigma_0 \notin \sigma_0, \sigma_0 \notin \epsilon \implies q$ after $\sigma_0 \notin E(\sigma_0 \cup \{q\})$. Then, we consider two cases:

- If $E(\sigma_0 \cup \{q\}) \notin E(\sigma_0 \cup \{q\})$, then $\text{Reach}(\sigma_0 \cup \{q\}) \notin E$, meaning that $E(\sigma_0 \cup \{q\}) \notin \varphi$.

- Otherwise, since $E$ is compliant, there exists $\sigma_2 \in \sigma_0 \cup \{q\}$ and $\sigma_0 \in \sigma_0 s.t. \sigma_2 \notin \epsilon$, $\sigma_2 \notin \epsilon$, and $E(\sigma_0 \cup \{q\}) = E(\sigma_0 \cup \{q\}) = \sigma_0 \cup \{q\}$. Let us consider $q' = q$ after $\sigma_0, \sigma_2 \notin E(\sigma_2) \cup I(\sigma_2)$, because otherwise, $q = \text{Reach}(\sigma_0 \cup \{q\}) \notin E(\sigma_0 \cup \{q\})$, which is absurd.

Thus, in both cases, there exists $\sigma_0 \in \Sigma^*$ s.t. $E(\sigma_0 \cup \{q\}) \notin \varphi$.

Thus, if $E$ is an enforcement function s.t. there exists $\sigma \in \text{Pre}(\varphi)$, and $\sigma \in \Sigma^*$ is compliant ($E$, $E(\sigma, \varphi)$), $E(\sigma) = E(\sigma, \varphi)$, and $|E(\sigma, \varphi)| > |E(\sigma, \varphi)|$, then there exists $\sigma_0 \in \Sigma^*$ s.t. $E(\sigma_0 \cup \{q\}) \notin \varphi$. This means that $E_\varphi$ is optimal in $\text{Pre}(\varphi)$.

**Proposition 5. The output of the enforcement monitor $E$ for input $\sigma$ is $E_\varphi(\sigma)$.**

**Proof.** Let us introduce some notation for this proof: for a word $w \in \Gamma^*$, we note $\text{input}(w) = \Pi_1(w(1)) \Pi_2(w(2)) \ldots \Pi_n(w(|w|))$, the word obtained by concatenating the first members (the inputs) of $w$. In a similar way, we note $\text{output}(w) = \Pi_1(w(1)) \Pi_2(w(2)) \ldots \Pi_n(w(|w|))$, the word obtained by concatenating the third members (the outputs) of $w$. Since all configurations are not reachable from $q_0$, for $w \in \Gamma^*$, we note $\text{Reach}(w) = w$ whenever $w_0^* \triangleright_w w$, and $\text{Reach}(w) = \perp$ if such a $w$ does not exist. We also define the Rules function as follows:

$$
\text{Rules : } \begin{cases}
\Sigma^* & \rightarrow & \Gamma^* \\
\sigma & \rightarrow & \text{max}_\Sigma\{\{w \in \Gamma^* | \text{input}(w) = \sigma \land \text{Reach}(w) \neq \perp\}\}
\end{cases}
$$

For a word $\sigma \in \Sigma^*$, $\text{Rules}(\sigma)$ is the trace of the longest valid run in $\Sigma^*$, i.e. the sequence of all the rules that can be applied with input $\sigma$. We then extend the definition of output to words in $\Sigma^*$: for $\sigma \in \Sigma^*$, output($\sigma$) = output(\text{Rules}(\sigma)). We also note $\epsilon$ the empty word of $\Sigma^*$, and $\epsilon^*$ the empty word of $\Gamma^*$. For $\sigma \in \Sigma^*$, let $P(\sigma)$ be the predicate: “$E_\varphi(\sigma) = \text{output}(\sigma) \land ((\sigma, \varphi) = \text{store}_\varphi(\sigma) \land \text{Reach}(\text{Rules}(\sigma)) = (q, \sigma^*) \implies (q = \text{Reach}(\sigma) \land \sigma_0 = \sigma^*)$”.

Let us prove by induction that for all $\sigma \in \Sigma^*$, $P(\sigma)$ holds.

- **Induction basis:** $E_\varphi(\epsilon) = \epsilon = \text{output}(\epsilon)$. Moreover, store$_{\varphi}(\epsilon) = (\epsilon, \epsilon)$, and $\text{Reach}(\epsilon^*) = q_0^\epsilon$. Therefore, as $q_0^\epsilon = (q_0, \epsilon)$, $P(\epsilon)$ holds, because $\text{Reach}(\epsilon) = q_0$.

- **Induction step:** Let us suppose now that for some $\sigma \in \Sigma^*$, $P(\sigma)$ holds. Let us consider $\sigma_1, \sigma_2$, store$_\varphi(\sigma_1), q = \text{Reach}(\sigma_0), a \in \Sigma$, and $(\sigma_1, \sigma_2) = \text{store}_\varphi(\sigma_0)$. Let us prove that $P(\sigma)$ holds.
Since $P(\sigma)$ holds, Reach(Rules($\sigma$)) = $(q, \sigma_q)$ and $\sigma_s = \text{output}(\sigma)$. We consider two cases:

- $a \in \Sigma_a$. Then, considering $\sigma'_s = (\sigma_s.a)^{-1}.\sigma_s = \sigma_s.a.\sigma'_s$. Since $a \in \Sigma_a$, rule pass-uncont can be applied: let us consider $q' = q$ after $a$. Then, $(q, \sigma_q) \xrightarrow{a/\text{pass-uncont}(a)/e} (q', \sigma_q)$. Then, if $\sigma'_s = \epsilon$, $G(q', \sigma_q) = \emptyset$ or $G(q', \sigma_q) = \{\epsilon\}$, meaning that no other rule can be applied, and thus $P(\sigma.a)$ would hold. Otherwise, $\sigma'_s \neq \epsilon$, and thus $\sigma'_s \in G(q', \sigma_q)$, meaning that $G(q', \sigma_q) \neq \emptyset$ and $G(q', \sigma_q) \neq \{\epsilon\}$, thus rule dump($\sigma_s(1)$) can be applied. Since $\sigma'_s \leq \sigma_s$, $\sigma'_s(1) = \sigma_s(1)$, thus if $q_1 = q'$ after $\sigma_s(1)$, $q_1 = q'$ after $\sigma_s(1)$.

- $a \in \Sigma_\omega$. Then, considering $\sigma''_s = \sigma^{-1}_s.\sigma_1 = \sigma_s.\sigma''_s$. Since $a \in \Sigma_\omega$, it is possible to apply the store-cont rule, and $(q, \sigma_q)$ after $a/\text{store-cont}(a)/e = (q, \sigma_q.a)$. Then as in the case where $a \in \Sigma_a$, rule dump can be applied $|\sigma''_s|$ times, meaning that the configuration reached would then be $(q$ after $(\sigma.s.a)(1).\cdot\cdot\cdot(\sigma.s.a)(|\sigma''_s|)., (\sigma.s.a)(|\sigma''_s| + 2).\cdot\cdot\cdot(\sigma.s.a)(|\sigma_s|))$. Since $\sigma''_s \leq \sigma_s$, $(\sigma.s.a)(1).\cdot\cdot\cdot(\sigma.s.a)(|\sigma''_s|) = \sigma''_s$, thus Reach(Rules($\sigma.s.a$)) = $(q$ after $\sigma''_s, \sigma''_s^{-1}, (\sigma.s.a))$. Moreover, output($\sigma.s.a$) = output($\sigma.s.a.\sigma''_s, \sigma.s.a) = (\text{Reach}(\sigma.s.a.\sigma''_s, \sigma.s.a) = (\text{Reach}(\sigma.s.a), \sigma.d_a)$.

Thus, if $a \in \Sigma_a$, $P(\sigma.s.a)$ holds.

Thus, if $a \in \Sigma_\omega$, $P(\sigma.s.a)$ holds. This means that $P(\sigma) \implies P(\sigma.s.a)$. Thus, by induction on $a$, for all $a \in \Sigma^*$, $P(\sigma)$ holds. In particular, for all $a \in \Sigma^*$, $E_{\omega}(\sigma) = \text{output}(\sigma)$.

A.2. Proofs for the Timed Setting

**Proposition 6.** $E_{\omega}$ as defined in Definition 16 is an enforcement function, as per Definition 16.

**Proof.** For $a \in \text{tw}(\Sigma)$, let $P(\sigma)$ be the predicate: "\(\forall t \in \mathbb{R}_{\geq 0}, \forall t' \geq t, E_{\omega}(\sigma, t) \leq E_{\omega}(\sigma, t')\)." Let us show by induction that for all $a \in \text{tw}(\Sigma)$, $P(\sigma)$ holds.

**Induction basis:** $\sigma = \epsilon$. Then, let us consider $t \in \mathbb{R}_{\geq 0}$, and $t' \geq t$. Then, $E_{\omega}(\epsilon, t) = \epsilon \leq \epsilon = E_{\omega}(\epsilon, t')$.

Thus, $P(\epsilon)$ holds.

**Induction step:** let us suppose that, for $a \in \text{tw}(\Sigma)$, $P(\sigma)$ holds. Let us consider $(t'', a)$ s.t. $\sigma.(t'', a) \in \text{tw}(\Sigma), t \in \mathbb{R}_{\geq 0}$, and $t' \geq t$.

- If $t \geq t''$, then let us consider $(\sigma_s, \sigma_b, \sigma_c) = \text{store}_{e}(\sigma, t''), (\sigma_{d_1}, \sigma_{d_2}, \sigma_{c_1}) = \text{store}_{e}(\sigma.(t'', a), t)$, and $(\sigma_{d_2}, \sigma_{d_2}) = \text{store}_{e}(\sigma.(t'', a), t')$. Then, $E_{\omega}(\sigma.(t'', a), t) = \sigma_{d_1}$ and $E_{\omega}(\sigma.(t'', a), t') = \sigma_{d_2}$.

- If $a \in \Sigma_a$, then considering $t_1$ as defined in Definition 16, $t_1 = \min\{|t_0 | t_0 \geq t'' \wedge G(\text{Reach}(\sigma.s.(t'', a), t_0), \Pi_{e}(\text{nobs}(\sigma.s.(t'', a)))) \neq \emptyset\}$.

- If $a \in \Sigma_\omega$, then considering $t_1$ as defined in Definition 16, $t_1 = \min\{|t_0 | t_0 \geq t'' \wedge G(\text{Reach}(\sigma.s.(t'', a), t_0), \Pi_{e}(\text{nobs}(\sigma.s.(t'', a)))) \neq \emptyset\}$.

- Case 1: $t \geq t''$, then $t' \geq t_1$, thus $\min\{|t_1 | t_1 \} = t_1$. Thus, $\sigma_{d_1} = \sigma_{d_2}$.

- Case 2: $t < t''$. Then, $\text{nobs}(\sigma.s.(t'', a), t) = (t, \sigma_{d_1}, \sigma_{d_2}) = \emptyset$. Then, $\sigma_{d_1} = \sigma_{d_2}$.
Thus, if \( t' \geq t \geq t'' \) and \( a \in \Sigma_n \), \( P(\sigma) \implies E_\varphi(\sigma(t'',a),t) \equiv E_\varphi(\sigma(t'',a),t') \).

- Otherwise, \( a \in \Sigma_n \), and then considering \( t_2 \) as defined in Definition 16, \( t_2 = \min\{t_0 \in \mathbb{R}_{\geq 0} \mid t_0 \geq t'' \land G(Reach(\sigma,s_{t_0})), \Pi_\Sigma(nobs(\sigma,t''))(\sigma,a) \neq \emptyset\} \). Then, \( \sigma_{a_1} = \min_{\max_{\varphi}} \{G(Reach(\sigma,s_{t_2})), \Pi_\Sigma(nobs(\sigma,t''))(\sigma,a) \cup \{\varphi\}\} + \min\{\{t_2\}, t_2\} \).

- Case 1: \( t \geq t_2 \). Since \( t' \geq t \geq t_2 \), meaning that \( \min\{\{t, t_2\}\} = \min\{\{t', t_2\}\} = t_2 \), and thus \( \sigma_{a_1} = \sigma_{a_2} \). It follows that \( \sigma_{a_1} = \sigma_s \circ \sigma \circ \sigma_{a_2} \), \( \sigma_s \circ \sigma \circ \sigma_{a_2} = \sigma_{a_2} \).

- Case 2: \( t < t_2 \). Then, \( G(Reach(\sigma,s_{t_{t_2}})), \Pi_\Sigma(nobs(\sigma,t''))(\sigma,a) = \emptyset \), meaning that \( \sigma_{a_1} = \epsilon \). Thus, \( \sigma_{a_1} = \sigma_s \circ \sigma \circ \sigma_{a_2} \).

Thus, if \( t' \geq t \geq t'' \) and \( a \in \Sigma_n \), \( P(\sigma) \implies E_\varphi(\sigma(t'',a),t) \equiv E_\varphi(\sigma(t'',a),t') \).

Therefore, if \( t' \geq t \geq t'' \), for all \( a \in \Sigma \), \( P(\sigma) \implies E_\varphi(\sigma(t'',a),t) \equiv E_\varphi(\sigma(t'',a),t') \).

- If \( t' < t'' \), then \( t < t' \), and \( \sigma(\sigma(t'',a),t) = \sigma(\sigma(\sigma(t''',a),t)),t) = \sigma(\sigma(\sigma(t''',a),t'),t) = \sigma(\sigma(t'',a),t') \).

- If \( t < t' \), then \( \sigma(\sigma(t'',a),t) = \sigma(\sigma(\sigma(t',a),t),t) \).

Let \( \sigma_s, \sigma_{a_1}, \sigma_{a_2} = \sigma_{a_1} \circ \sigma_s \circ \sigma_{a_2} \).

Since \( \sigma_s \circ \sigma \circ \sigma_{a_2} = \sigma_{a_1} \), \( \sigma_s \circ \sigma \circ \sigma_{a_2} = \sigma_{a_1} \).

Thus, if \( t' \leq t \), then \( \sigma(\sigma(t'',a),t) \equiv E_\varphi(\sigma(\sigma(t',a),t),t) \).

Consequently, in all cases, if \( t \leq t' \), then \( P(\sigma) \implies E_\varphi(\sigma(t'',a),t) \equiv E_\varphi(\sigma(t',a),t') \).

By induction, for all \( \sigma \in tw(\Sigma) \), \( P(\sigma) \) holds. Thus, for all \( \sigma \in tw(\Sigma) \), for all \( t \in \mathbb{R}_{\geq 0} \), for all \( t' \geq t \), \( E_\varphi(\sigma(t'',a),t) \equiv E_\varphi(\sigma(t',a),t) \).

Now, let us consider \( \sigma \in tw(\Sigma) \), and \( (t,a) \) s.t. \( \sigma(t,a) \in tw(\Sigma) \). Then, if \( \sigma_s, \sigma_{a_1}, \sigma_{a_2} = \sigma_{a_1} \circ \sigma_s \circ \sigma_{a_2} \), \( \sigma_s \circ \sigma \circ \sigma_{a_2} = \sigma_{a_1} \).

Thus, \( \sigma_s \circ \sigma \circ \sigma_{a_2} = \sigma_{a_1} \).

This holds because, since \( \sigma(t,a) \in tw(\Sigma) \), \( \sigma(\sigma(t',a),t) \).

Thus, for all \( \sigma \in tw(\Sigma) \), for all \( t \in \mathbb{R}_{\geq 0} \) and \( t' \geq t \), \( E_\varphi(\sigma(t'',a),t) \equiv E_\varphi(\sigma(t',a),t) \).

This means that \( E_\varphi(\sigma(t'',a),t) \equiv E_\varphi(\sigma(t',a),t) \).

Lemma 6. \( \forall t \in \mathbb{R}_{\geq 0}, \forall \sigma \in tw(\Sigma), (\sigma \notin \text{Pre}(\varphi,t) \land (\sigma_s, \sigma_{a_1}, \sigma_{a_2} = \sigma_{a_1} \circ \sigma_s \circ \sigma_{a_2}) \implies \sigma = \sigma_s \circ \sigma \circ \sigma_{a_2} = \sigma_s \circ \sigma \circ \sigma_{a_2} \).

Proof. For \( \sigma \in tw(\Sigma) \), let \( P(\sigma) \) be the predicate “\( \forall t \geq \text{time}(\sigma), (\sigma \notin \text{Pre}(\varphi,t) \land (\sigma_s, \sigma_{a_1}, \sigma_{a_2} = \sigma_{a_1} \circ \sigma_s \circ \sigma_{a_2}) \implies \sigma = \sigma_s \circ \sigma \circ \sigma_{a_2} \)”. Let us prove by induction that for all \( \sigma \in tw(\Sigma), P(\sigma) \) holds.

- Induction basis: for \( \sigma = \epsilon \), let us consider \( t \in \mathbb{R}_{\geq 0} \). Then, \( \text{store}_\varphi(\epsilon,t) = (\epsilon, \epsilon, \epsilon) \). Considering that \( \epsilon \in \text{time}(\Sigma) \), and \( \epsilon = \Pi_\Sigma(\epsilon,\Sigma) \).

- Induction step: suppose that for \( \sigma(s,t), P(\sigma) \) holds. Let us consider \( (t',a) \) s.t. \( \sigma(t',a) \in tw(\Sigma) \), and \( t' \geq t \). Let us also consider \( \sigma_s, \sigma_{a_1}, \sigma_{a_2} = \sigma_{a_1} \circ \sigma_s \circ \sigma_{a_2} \).

Then, if \( \sigma(t',a) \in \text{Pre}(\varphi,t), P(\sigma(t',a)) \) trivially holds. Thus, let us suppose that \( \sigma(t',a) \notin \text{Pre}(\varphi,t) \).

Since \( \sigma \notin \text{Pre}(\varphi,t) \) and \( t' \geq t \), it follows that \( \sigma \notin \text{Pre}(\varphi,t') \). By induction hypothesis, this means that \( \sigma_{a_1} = \sigma_{a_2} = \epsilon \), and \( \sigma_s = \Pi_\Sigma(\epsilon,\Sigma) \).

Then, since \( \sigma(t',a) \notin \text{Pre}(\varphi,t) \), following the definition of \( \text{Pre}(\varphi,t) \), this means that for all \( t'' \leq t \), \( \text{G}(\text{Reach}(\text{obs}(\sigma(t',a),t''), \Pi_\Sigma(\text{obs}(\sigma(t',a),t''), \text{obs}(\sigma(t',a),t'')) \equiv \emptyset \).

[End of proof]
Optimal Enforcement of (Timed) Properties with Uncontrollable Events

Suppose now that for the definition of $S(\cdot, a)$, we have $G(Reach(\sigma_0, t), \Pi(\cdot, a, t) = \sigma(\cdot, t, a))$. Then, there are two cases:

- **Case 1**: $a \in \Sigma_a$. Then, $(\sigma, t, a))_{\Sigma_a} = \sigma_{\Sigma_a}(\cdot, t, a) = \sigma_s(\cdot, t, a)$, and $\Pi(\cdot, t, a)_{\Sigma_a} = \Pi(\Sigma, \cdot, t, a) = \Pi(\Sigma, \cdot, t, a) = \Pi(\Sigma, \cdot, t, a)$. Thus, $P(\sigma, t, a))$ holds if $a \in \Sigma_a$.

- **Case 2**: $a \notin \Sigma_a$. Then, $(\sigma, t, a))_{\Sigma_a} = \sigma_{\Sigma_a}(\cdot, t, a) = \sigma_s(\cdot, t, a)$, and $\Pi(\cdot, t, a)_{\Sigma_a} = \Pi(\Sigma, \cdot, t, a) = \Pi(\Sigma, \cdot, t, a)$. Thus, $P(\sigma, t, a))$ holds if $a \in \Sigma_a$.

By induction, for all $\sigma \in tw(\Sigma)$, $P(\sigma)$ holds. Thus, for all $\sigma \in tw(\Sigma)$, for all $t \in \mathbb{R}_{\geq 0}$, if $(\sigma_s, \sigma_a, \sigma_e) = store_p(\sigma, t)$ and $(\sigma_t, t, \varphi) \notin \mathcal{P}(\sigma)$, then $\sigma = \sigma_{\Sigma_a}$, $\sigma_b = \epsilon$, and $\sigma_c = \Pi(\sigma_{\Sigma_a})$.

**Lemma 7.** $\forall \sigma \in \Sigma_\sigma, \forall a \in \Sigma_a, I(\sigma) \subseteq I(\sigma_a)$.

**Proof.** For $\sigma \in \Sigma_\sigma$, let $P(\sigma)$ be the predicate “$\forall a \in \Sigma_a, I(\sigma) \subseteq I(\sigma_a)$”. Let us show by induction that $P(\sigma)$ holds for all $\sigma \in \Sigma_\sigma$.

- **Induction basis:** let us consider $a \in \Sigma_a$. Then, $I(\epsilon) = \emptyset \subseteq I(\epsilon)$.

- **Induction step:** suppose now that for $\sigma \in \Sigma_\sigma$, for all $\sigma' \in \Sigma_\sigma$, s.t. $|\sigma'| \leq |\sigma|$, $P(\sigma')$ holds. Let us then consider $a \in \Sigma_a$, $\sigma' \in \Sigma_a$, and $(h, \sigma_a) \in \Sigma_a \times \Sigma_a$, s.t. $h, \sigma_0 = \sigma_a$, and $\sigma_0$ exist because $\sigma_a \neq \sigma$. Then, $I(\sigma, a') \equiv I(h, \sigma_0, a') = \text{Pred}_a(S(\sigma_0, a') \cup I(\sigma_0, a'))$, and $I(\sigma, a) = I(h, \sigma_0) = \text{Pred}_a(S(\sigma_0) \cup I(\sigma_0))$. Following the definition of $S(\sigma_0) \subseteq S(\sigma_0, a')$. Moreover, by induction hypothesis, since $|\sigma_0| \leq |\sigma|$, $P(\sigma_0)$ holds, meaning that $I(\sigma_0) \subseteq I(\sigma_0, a')$. Thus, $S(\sigma_0) \cup I(\sigma_0) \subseteq S(\sigma_0, a') \cup I(\sigma_0, a')$. It follows that $I(\sigma, a) = \text{Pred}_a(S(\sigma_0) \cup I(\sigma_0)) \subseteq \text{Pred}_a(S(\sigma_0, a') \cup I(\sigma_0, a'))$ = $I(\sigma, a)$. Thus, for all $\sigma' \in \Sigma_a$, $I(\sigma, a) \subseteq I(\sigma, a')$, meaning that $P(\sigma, a)$ holds.

By induction, $P(\sigma)$ holds for every $\sigma \in \Sigma_a$, meaning that for all $\sigma \in \Sigma_\sigma$, for all $a \in \Sigma_a$, $I(\sigma) \subseteq I(\sigma_a)$.

**Lemma 8.** $\forall q \in Q, \forall \sigma \in \Sigma_\sigma, (q \in S(\sigma)) \implies (\forall u \in \Sigma_u, q \text{ after } (0, u) \in S(\sigma) \cup I(\sigma))$.

**Proof.** For $\sigma \in \Sigma_\sigma$, let $P(\sigma)$ be the predicate “$\forall q \in Q, (q \in S(\sigma)) \implies (\forall u \in \Sigma_u, q \text{ after } (0, u) \in S(\sigma) \cup I(\sigma))$”. Let us show by induction on $\sigma$ that $P(\sigma)$ holds for every $\sigma \in \Sigma_\sigma$.

- **Induction basis:** let us consider $q \in S(\epsilon)$. Then, for all $u \in \Sigma_u$, since $(0, u) \in tw(\Sigma)$, considering the definition of $S(\epsilon)$, $q$ after $u \in S(\epsilon)$. Thus, $q \in S(\epsilon) \cup I(\epsilon)$. Thus, $P(\epsilon)$ holds.

- **Induction step:** let us suppose that for $\sigma \in \Sigma_\sigma$, $P(\sigma)$ holds. Let us consider $a \in \Sigma_a$ and $q \in S(\sigma, a)$. Then, considering the definition of $S(\sigma, a)$, two cases are possible:

  - Either $q \in S(\sigma)$, and then, by induction hypothesis, for all $u \in \Sigma_u$, $q$ after $u \in S(\sigma) \cup I(\sigma)$.

  - $q \in S(\sigma, a) \setminus S(\sigma)$, and then, since $(S(\sigma, a) \setminus S(\sigma)) \cap uP \text{Pred}_a(S(\sigma, a) \setminus S(\sigma))\cup I(\sigma, a)) = \emptyset$, it follows that if $u \in \Sigma_u$, $q$ after $u \in (S(\sigma, a) \setminus S(\sigma)) \cup I(\sigma, a)$.

In both cases, for all $u \in \Sigma_u$, $q$ after $u \in S(\sigma, a) \cup I(\sigma, a)$, meaning that $P(\sigma, a)$ holds. Thus, by induction, for all $\sigma \in \Sigma_\sigma$, $P(\sigma)$ holds. Thus, for all $\sigma \in \Sigma_\sigma$, for all $q \in S(\sigma)$, for all $u \in \Sigma_u$, $q$ after $u \in S(\sigma) \cup I(\sigma)$.
Lemma 9. For all $\sigma \in \Sigma_\ast$, for all $q \in Q$, $(q \in S(\sigma) \cup I(\sigma)) \implies (G(q, \sigma) \neq \emptyset)$.

Proof. For $\sigma \in \Sigma_\ast$, let $P(\sigma)$ be the predicate "$\forall q \in Q, (q \in S(\sigma) \cup I(\sigma)) \implies (G(q, \sigma) \neq \emptyset)$". Let us then prove by induction on $\sigma$ that $P(\sigma)$ holds for every $\sigma \in \Sigma_\ast$.

--- Induction basis: let us consider $q \in S(\epsilon) \cup I(\epsilon)$. Since $I(\epsilon) = \emptyset$, this means that $q \in S(\epsilon)$. Then, $\epsilon$ satisfies $\epsilon \subseteq \Pi_2(\epsilon)$. Moreover, since $S(\epsilon) \subseteq F_G$, $q$ after $\epsilon = q \in F_G$, and for all $t \in \mathbb{R}_{\geq 0}$, $q$ after $(\epsilon, t)$ is in $S(\epsilon)$, because otherwise there would exist $\sigma_a \in \text{tw}(\Sigma_a)$ s.t. $q$ after $(\epsilon, t)$ after $\sigma_a \notin F_G$, meaning that $q$ after $(\sigma_a + t) \notin F_G$, and thus $q$ would not be in $S(\epsilon)$. Thus, $\epsilon \in G(q, \epsilon)$. This means that $G(q, \epsilon) \neq \emptyset$, and thus that $P(\epsilon)$ holds.

--- Induction step: let us suppose that for $n \in \mathbb{N}$, for all $\sigma \in \Sigma_\ast$, $|\sigma| \leq n \implies P(\sigma)$. Let us consider $\sigma \in \Sigma_\ast$ s.t. $|\sigma| = n$, $a \in \Sigma_e$, and $q \in S(\sigma.a) \cup I(\sigma.a)$.

- If $q \in I(\sigma.a)$, let us consider $(i, \sigma_0) \in \Sigma_e \times \Sigma_\ast$ s.t. $\sigma.a = h.\sigma_0$. Then, $q \in I(h.\sigma_0) = \text{Pred}_{i}(S(\sigma_0) \cup I(\sigma_0))$, and since $|\sigma_0| = |\sigma| = n \leq n$, by induction hypothesis, $G(q \text{ after } (0, h, \sigma_0)) \neq \emptyset$. Let us consider $w \in G(q \text{ after } (0, h, \sigma_0)).$ Then, $(0, h).w$ satisfies $\Pi_2((0, h).w) \leq h.\sigma_0$. $q$ after $(0, h).w = q$ after $(0, h)$ after $w \in F_G$, and for all $t \in \mathbb{R}_{\geq 0}$, $q$ after $(0, h, w, t) = q$ after $(0, h)$ after $(w, t) \in S(\Pi_2((0, h,w)^{-1})).$ Thus, $(0, h).w \in G(q, h.\sigma_0) = G(q, \sigma.a)$. Thus, $G(q, \sigma.a) \neq \emptyset$.

- If $q \in S(\sigma.a)$, then there are again two cases:
  - If $q \in S(\sigma)$, then by induction hypothesis, $G(q, \sigma) \neq \emptyset$. Since $G(q, \sigma) \subseteq G(q, \sigma.a)$, it follows that $G(q, \sigma.a) \neq \emptyset$.
  - Otherwise, $q \in X \cup Y$, where $X$ and $Y$ are defined in the definition of $S(\sigma.a)$.
    - If $q \in X$, then there exists $i \in \sigma(\sigma.a)$ and $\delta \in \mathbb{R}_{\geq 0}$ s.t. $q$ after $(\epsilon, \delta) = i$, and for all $t \leq \delta$, $q$ after $(\epsilon, t) \in X \subseteq S(\sigma.a)$. Since $i \in I(\sigma.a)$, we showed previously that $G(i, \sigma.a) \neq \emptyset$. Let us consider $w \in G(i, \sigma.a)$. Then, $w + i, \delta$ satisfies $\Pi_2(w + i, \delta) \leq \sigma.a$, $q$ after $(w + i, \delta)$ is $i$ after $w \in F_G$, and for all $t \in \mathbb{R}_{\geq 0}$, if $t < \delta$, then $q$ after $(w + i, \delta, t) = q$ after $(\epsilon, t) \in X \subseteq S(\sigma.a)$, otherwise, $q$ after $(w + i, \delta, t) = i$ after $(w, t - \delta) \in S(\sigma.a).$ Thus, $w + i, \delta \in G(q, \sigma.a)$. Thus, $G(q, \sigma.a) \neq \emptyset$.
    - Otherwise, $q \in Y$, and then $\epsilon$ satisfies $\Pi_2(\epsilon) \leq \sigma.a$, $q$ after $\epsilon \in F_G$, and for all $t \in \mathbb{R}_{\geq 0}$, $q$ after $(\epsilon, t) \in \text{up}(q) \subseteq \text{up}(Y) = Y \subseteq S(\sigma.a)$. Thus, $\epsilon \in G(q, \sigma.a)$. Thus, $G(q, \sigma.a) \neq \emptyset$. Thus, for all $q \in S(\sigma.a) \cup I(\sigma.a)$, $G(q, \sigma.a) \neq \emptyset$. Thus, $P(\sigma)$ holds. By induction on $\sigma$, $P(\sigma)$ holds for ever $\sigma \in \Sigma_\ast$, meaning that for all $\sigma \in \Sigma_\ast$, for all $q \in S(\sigma) \cup I(\sigma)$, $G(q, \sigma) \neq \emptyset$.

Proposition 7. $E_\varphi$ is sound with respect to $\varphi$ in $\text{Pre}(\varphi)$ as per Definition 12.

Proof. Notation from Definition 16 is to be used in this proof:

For $\varphi$, $\kappa_\varphi(q, w) = \min_{\text{lex}}\max\{G(q, w) \cup \{\epsilon\}\}$, for $q \in Q$ and $w \in \Sigma_\ast$,

buffer\_\varphi = \Pi_2(\text{nobs}(\sigma_x, t'))(\sigma_x),

t_1 = \min\{t' \in \mathbb{R}_{\geq 0} \mid t' \geq t \wedge G(\text{Reach}(\sigma_x, (t', a), t'), \text{buffer\_\varphi}) \neq \emptyset \cup \{+\infty\})

\sigma'_x = \kappa_\varphi(\text{Reach}(\sigma_x, (t', a), \min\{t, t_1\}), \text{buffer\_\varphi} + \min\{t, t_1\})

\sigma''_x = \Pi_2(\sigma'_x)^{-1}(\text{buffer\_\varphi}).

t_2 = \min\{t'' \in \mathbb{R}_{\geq 0} \mid t'' \geq t \wedge G(\text{Reach}(\sigma_x, t''), \text{buffer\_\varphi}) \neq \emptyset \cup \{+\infty\})

\sigma'_x = \kappa_\varphi(\text{Reach}(\sigma_x, \min\{t, t_2\}), \text{buffer\_\varphi} + \min\{t, t_2\})

\sigma''_x = \Pi_2(\sigma''_x)^{-1}(\text{buffer\_\varphi}).
Induction step: Optimal Enforcement of (Timed) Properties with Uncontrollable Events

—Induction basis: for \( \sigma = \epsilon \), let us consider \( t \in \mathbb{R}_{\geq 0} \).

—Case 1: \( \sigma \in \text{Pre}(\varphi, t) \). Then, \( P(\sigma, t) \) trivially holds.

—Case 2: \( \sigma \notin \text{Pre}(\varphi, t) \). Then, there exists \( t' \leq t \) s.t. \( G(\text{Reach}(\varphi, t')) \), \( \epsilon \neq \emptyset \), meaning that \( G(\text{Reach}(\epsilon, t'), \epsilon) \neq \emptyset \), and \( \text{Reach}(\epsilon) \in F_G \). Since \( E_{\varphi}(\epsilon) = \epsilon \), and \( \text{Reach}(\epsilon) \in F_G \), \( E_{\varphi}(\epsilon) = \emptyset \). Thus, because \( \text{store}_e(\epsilon) = (\epsilon, \epsilon), P(\epsilon, t) \) holds.

Thus, in both cases, \( P(\varphi, t) \) holds, meaning that \( P(\epsilon, t) \).

—Induction step: suppose that for \( \sigma \in \text{tw}(\Sigma) \), \( P(\sigma) \) holds. Let us consider \((t', a) \text{ s.t. } \sigma, (t', a) \in \text{tw}(\Sigma) \), and \( t \geq t' = \text{time}(\sigma, (t', a)) \). Let us also consider \((\sigma_1, \sigma_2, \sigma_c) = \text{store}_c(\sigma, (t', a)), (t) \).

—Case 1: \( \sigma, (t', a) \notin \text{Pre}(\varphi, t) \). Then, \( P(\sigma, (t', a), t) \) trivially holds.

—Case 2: \( \sigma, (t', a) \in \text{Pre}(\varphi, t) \). Then, \( \sigma \notin \text{Pre}(\varphi, t) \), therefore, following the definition of \( G(\text{Reach}(\sigma, (t', a))) \), \( \sigma \) holds.

—Case 3: \( \sigma, (t', a) \in \text{Pre}(\varphi, t) \) and \( \sigma \notin \text{Pre}(\varphi, t) \). Then, consider \( w_0 = \text{obs}(\sigma, t_0) = t' \). By the induction hypothesis, since \( \sigma \in \text{Pre}(\varphi, t'), E_{\varphi}(\sigma) = \emptyset, w_0 \in G(\text{Reach}(\sigma, t'), P(\sigma, (t', a), t)) \).

—Case 3: \( \sigma, (t', a) \in \text{Pre}(\varphi, t) \) and \( \sigma \notin \text{Pre}(\varphi, t) \). Then, consider \( w_0 = \text{obs}(\sigma, t_0) = t' \). By the induction hypothesis, since \( \sigma \in \text{Pre}(\varphi, t'), E_{\varphi}(\sigma) = \emptyset, w_0 \in G(\text{Reach}(\sigma, t'), P(\sigma, (t', a), t)) \).
Induction step: $E$.

Thus, in all cases, for all $t$, $P(\sigma, (t', a), t)$ holds. This means that $P(\sigma) \Rightarrow \forall t \geq t', P(\sigma, (t', a), t)$. Thus, $P(\sigma) \Rightarrow P(\sigma, (t, a), t)$. By induction, for all $\sigma \in tw(\Sigma)$, $P(\sigma)$ holds. In particular, for all $(\sigma, t) \in Pre(\varphi)$, $E_\varphi(\sigma) \models \varphi$. This means that $E_\varphi$ is sound in $Pre(\varphi)$.

---

**Proposition 8.** $E_\varphi$ is compliant, as per **Definition 13**.

Proof. For $\sigma \in tw(\Sigma)$, let $P(\sigma)$ be the predicate: “$\forall t \geq \text{time}(\sigma), (\sigma_x, \sigma_y, \sigma_z) = \text{store}_\varphi(\sigma, t) \Rightarrow \sigma_{x|\Sigma_x} = \sigma_{y|\Sigma_y} \land P_\Sigma(\sigma_{y|\Sigma_y}, \text{obs}(\sigma_y, t)). \sigma_z = P(\sigma_{y|\Sigma_y}) \land \sigma_{y|\Sigma_y} \preceq \sigma_{x|\Sigma_x}$.” Let us prove by induction that for all $\sigma \in tw(\Sigma)$, $P(\sigma)$ holds.

---

**Induction basis:** for $\sigma = \epsilon$, $\text{store}_\varphi(\epsilon) = (\epsilon, \epsilon, \epsilon)$, and $\epsilon_{x|\Sigma_x} = \epsilon_{y|\Sigma_y} = P(\epsilon) = \epsilon$. Thus, $P(\epsilon)$ trivially holds.

**Induction step:** suppose now that for some $\sigma \in tw(\Sigma)$, $P(\sigma)$ holds. Let us consider $(t', a) \in tw(\Sigma)$, $t \geq \text{time}(\sigma)$, $(\sigma_x, \sigma_y, \sigma_z) = \text{store}_\varphi(\sigma, t')$, and $(\sigma_x, \sigma_y, \sigma_z) = \text{store}_\varphi(\sigma, (t', a), t)$. Then, by induction hypothesis, $\sigma_{x|\Sigma_x} = \sigma_{y|\Sigma_y}, P_{\Sigma}(\sigma_{y|\Sigma_y}), \sigma_z = P(\sigma_{y|\Sigma_y})$, and $\sigma_{y|\Sigma_y} \preceq \sigma_{x|\Sigma_x}$.

$a \in \Sigma_x$. By construction, $\sigma_x$ satisfies $P_{\Sigma}(\sigma_x) \Leftrightarrow P_\Sigma(\sigma_{y|\Sigma_y}, \text{obs}(\sigma_y, t'). \sigma_z$ and $\sigma_d \neq \epsilon \Rightarrow \text{date}(\sigma_d(1)) \geq t'$.

**Projection on $\Sigma_x$:** Since $a \in \Sigma_x$, $\sigma_{x|\Sigma_x} = (\sigma_x, \sigma_y, \sigma_z) = \text{obs}(\sigma_d, t) |_{\Sigma_x}$. $\sigma_d \in tw(\Sigma)$, thus $\sigma_{x|\Sigma_x} = \sigma_{y|\Sigma_y}, (t', a) = \sigma_{x|\Sigma_x}, (t', a)$.

**Projection on $\Sigma_x$:** $P_\Sigma(\sigma_{y|\Sigma_y}, \text{obs}(\sigma_y, t'). \sigma_z$.

**Projection on $\Sigma_x$:** $P_{\Sigma}(\sigma_{y|\Sigma_y}, \text{obs}(\sigma_y, t'). \sigma_z$.

This means that if $a \in \Sigma_x$, $P(\sigma, (t', a))$ holds.

$a \in \Sigma_y$. By construction, $\sigma_y$ satisfies $P(\sigma_d(1)) \Leftrightarrow P_\Sigma(\sigma_{y|\Sigma_y}, \sigma_y, \sigma_z) = \epsilon$.

**Projection on $\Sigma_y$:** $\sigma_{y|\Sigma_y} = (\sigma_x, \sigma_y, \sigma_z) |_{\Sigma_y}$. Since $\sigma_d \in tw(\Sigma)$, $\sigma_{x|\Sigma_x} = \sigma_{y|\Sigma_y} = (\sigma_x, (t', a)) |_{\Sigma_y}$.

**Projection on $\Sigma_y$:** $P_{\Sigma}(\sigma_{y|\Sigma_y}, \text{obs}(\sigma_y, t'). \sigma_z$.

**Projection on $\Sigma_y$:** $P_{\Sigma}(\sigma_{y|\Sigma_y}, \text{obs}(\sigma_y, t'). \sigma_z$.

It follows that $P_{\Sigma}(\sigma_{y|\Sigma_y}, \sigma_z) = P(\sigma_{y|\Sigma_y}) \land P_{\Sigma}(\sigma_{y|\Sigma_y}, \sigma_z) = P(\sigma_{y|\Sigma_y})$. Moreover, as defined in **Definition 16**, $t_2 \geq t'$, and $t \geq t'$, thus $\text{min} \{t_1, t_2\} \geq t'$, which means that since there exists
Optimal Enforcement of (Timed) Properties with Uncontrollable Events

Thus if $a \in S_\sigma$, $P(\sigma, (t, a))$ holds.

Thus $P(\sigma) \Rightarrow P(\sigma, (t, a))$. By induction, for all $\sigma \in \text{tw}(\Sigma)$, for all $t \geq \text{time}(\sigma)$, $(\sigma, s, s_\sigma, s_\epsilon) = \text{store}_{\sigma}(s, t) \Rightarrow \sigma |_{S_\sigma} = \sigma |_{S_\epsilon} \cup \Pi_\epsilon(\sigma |_{S_\sigma}, \text{nobs}(s_\sigma, t)). s_\epsilon = \Pi_\epsilon(\sigma |_{S_\epsilon}, \text{nobs}(s_\sigma, t)).$ Thus $P_{\sigma}$ is compliant.

**Lemma 10.** $\forall x \in \Sigma_\sigma, \forall q \in Q.(q \notin \text{S}(\sigma)) \Rightarrow (\exists q_\epsilon \in \text{tw}(\Sigma_\sigma). q \text{ after } s_\sigma \notin F_\sigma \land (\forall t > 0. q \text{ after } s_\sigma, t \notin S(\sigma) \cup I(\sigma)) \land (\forall x_\sigma \notin \sigma, x_\epsilon \neq x \land q \text{ after } s_\epsilon \in S(\sigma) \cup I(\sigma))).$ We let show the contrapositive of the proposition, that is that for all $\sigma \in \Sigma_\sigma$, for all $q \in Q.(P(\sigma, q) \Rightarrow (q \in \text{S}(\sigma)).$

---If $\sigma = \epsilon$, let us consider $q \in Q$ s.t. $P(\epsilon, q)$ holds. Then, since $\epsilon \in \text{tw}(\Sigma_\sigma)$, $q$ after $\epsilon = q \in F_\sigma$, or there exists $t > 0 \text{ s.t. } q \text{ after } (\epsilon, t) \in S(\epsilon) \cup I(\epsilon)$. If the last condition holds, then $q \text{ after } (\epsilon, t) \in F_\sigma$, meaning that $q \in F_\sigma$. Thus, $q \in F_\sigma$.

Moreover, since $P(\epsilon, q)$ holds, for all $\sigma \in \text{tw}(\Sigma_\sigma)$, $q$ after $\epsilon$ s.t. $q \text{ after } (\epsilon, t) \in S(\epsilon) \cup I(\epsilon)$, meaning that $q \in F_\sigma$. Thus, $q \in F_\sigma$.

---If $\sigma \neq \epsilon$, there exists $(\sigma', a) \in \Sigma_\sigma \times \Sigma$ s.t. $\sigma = \sigma'.a$. Let us consider $q \in Q$ s.t. $P(\sigma, q)$ holds. Then, for all $\sigma \in \text{tw}(\Sigma_\sigma)$, $q$ after $\sigma$ s.t. $Q \text{ after } (\sigma', t) \in S(\sigma) \cup I(\sigma)$, or there exists $t > 0 \text{ s.t. } q \text{ after } (\sigma', t) \in S(\sigma) \cup I(\sigma)$. Let $X_\sigma$ and $Y_\sigma$ be s.t. $S(\sigma) = S(\sigma'.a)$. Then, $\forall x \in X_\sigma, \exists i \in \text{I}(\sigma'.a), \exists y \in \text{I}(\sigma).$

$s_\sigma \in \text{tw}(\Sigma_\sigma), t \in \text{R}$, $t \geq 0$, $s_\sigma = \epsilon \Rightarrow \forall x \in X_\sigma, s_\sigma \notin S(\sigma).$

Thus $s_\sigma \notin S(\sigma).$
and for all \( t < \delta + \delta', x \) after \((\epsilon, t)\) in \(X\). Moreover, \((X \cup Y) \cap u\text{Pred}(X \cup Y \cup I(\Sigma)) = \emptyset\) since \(Y = Y_h \cup Y_o \subseteq S(\sigma) \cup X_h, X \subseteq X_h \cup X_o,\) and \(X \cup Y = X_h \cup S(\sigma)\). This means that \(X \cup Y \subseteq S(\sigma)\), and since \(X_h \subseteq X \cup Y, X_o \subseteq S(\sigma)\). Since \( q = q \) after \((\epsilon, 0)\), with \( \epsilon \in t(w(\Sigma_0)) \) and \( t \in \mathbb{R}_{\geq 0}, q \in X_0,\) and thus \( q \in S(\sigma)\). Thus, if \( \sigma \neq \epsilon \) and \( q \in Q, P(\sigma, q) \implies q \in S(\sigma)\).

Thus, for all \( \sigma \in \Sigma_0^* \), for all \( q \in Q, P(\sigma, q) \implies q \in S(\sigma)\). Thus, the contrapositive also holds, meaning that for all \( \sigma \in \Sigma_0^* \), for all \( q \in Q, q \not\in S(\sigma) \implies \neg P(\sigma, q) \), that is \( \neg q \not\in S(\sigma) \implies (\exists \sigma_u \in t(w(\Sigma_0), q) \neg q \not\in F_c \land \forall t > 0, q \neg (\sigma_u, t) \not\in S(\sigma) \cup I(\sigma) \land \forall \sigma_u \neq \sigma, \sigma_u \neq \epsilon \implies q \neg (\sigma_u, t) \not\in S(\sigma) \cup I(\sigma))\).

**Proposition 9.** \( E_x \) is optimal in \( P(\varphi) \), as per Definition 14.

**Proof.** Let us consider \( E' : \mathcal{w}(\Sigma) \times \mathbb{R}_{\geq 0} \rightarrow \mathcal{w}(\Sigma) \), that is compliant with respect to \( \Sigma_0 \) and \( \Sigma_u \). Let us also consider \( \sigma \in \mathcal{w}(\Sigma) \), and \((t', a)\) s.t. \( \sigma(t', a) \in \mathcal{w}(\Sigma) \). Suppose now that \( \sigma(t') \in P(\varphi) \), \( E'(\sigma, t') = E_x(\sigma, t') \), and that \( E_{\Sigma_0}(\sigma(t', a)) \prec_d E'(\sigma(t', a)) \). Consider \( (\sigma_u, \sigma_d, \sigma_c) = \text{store}_{\Sigma}(\sigma, t') \), and \((\sigma_1, \sigma_d, \sigma_c) = \text{store}_{\Sigma}(\sigma(t', a), t)\), where \( t \) is s.t. \( \sigma_1 = E_x(\sigma(t', a)) \). Then, considering proof of soundness, since \( (\sigma, t') \in P(\varphi) \), \( \text{obs}(\sigma, t') \leftarrow t' \in \text{G(Reach}(\sigma, t'), \Pi_{\Sigma_0}(\text{obs}(\sigma, t'), \sigma)) \).

If \( a \in \Sigma_0 \), this means that \( \sigma_d \prec t' \in \text{G(Reach}(\sigma(t', a)), \Pi_{\Sigma_0}(\text{obs}(\sigma, t'), \sigma)) \). Let us consider \( q = \text{Reach}(\sigma(t', a), \sigma_1), \) and \( \text{buff} = \Pi_{\Sigma_0}(\text{obs}(\sigma, t'), \sigma_1) \). Then, \( \sigma_d \prec t' \prec \min_{\sigma_1}(\max_{\sigma_1}(G(q, \text{buff}))) \). \( E' \) is compliant with respect to \( \Sigma_0 \) and \( \Sigma_u \) thus, since \( E_{\Sigma_0}(\sigma, t') = E'(\sigma, t') \), there exists \( \sigma_d \in \mathcal{w}(\Sigma) \) such that \( E'(\sigma, t') = E'(\sigma(t', a)) \), \( \sigma_d \prec_a \sigma_1 \). Since \( E_x(\sigma(t', a), a) \prec_d E'(\sigma(t', a)) \), \( \sigma_d \prec_a \sigma_2 \) thus \( \sigma_d \prec t' \prec \sigma_d \prec a \sigma_2 \prec t' = w_{d_2}, \) meaning that \( w_{d_2} \not\in G(q, \text{buff}) \). Then, following the definitions of \( G \) and \( S \), there are some cases:

- \( \Pi_{\Sigma_0}(w_{d_2}) \not\in \text{buff} \). But, since \( E' \) is compliant, and \( E'(\sigma) = E_x(\sigma) \), this is not possible.
- \( q \prec_a \sigma_2 \not\in F_c, \) meaning that \( E'(\sigma(t', a)) \not\in \varphi \).

There exists \( t' \in \mathbb{R}_{\geq 0} \) s.t. \( q \prec_a (w_{d_2}, t') \not\in S(\Pi_{\Sigma_0}(\text{obs}(w_{d_2}, t'))^{-1}. \text{buff}) \). Let us then note \( \text{buff}_{d_2} = \Pi_{\Sigma_0}(\text{obs}(w_{d_2}, t'))^{-1}. \text{buff} \) and \( q_2 = q \prec_a (w_{d_2}, t') \). Then, following lemma 10, there exists \( \sigma_u \in \mathcal{w}(\Sigma_0) \) s.t. \( q_2 \prec_a \sigma_u \not\in F_c, \) for all \( q_2 \prec_a \sigma_u \not\in S(\text{buff}_{d_2}) \cup I(\text{buff}_{d_2}) \), and for all \( \sigma_u \prec_a \sigma_u \). Consider \( E'(\sigma(t', a), \sigma_u \prec_a t') = E'(\sigma(t', a), \sigma_u \prec_a t') = \text{obs}(w_{d_2}, t') \). \( \sigma_u \prec_a t' \), meaning that \( E'(\sigma(t', a)) \not\in \varphi \), or there exists \( \sigma_u \prec_a \sigma_u, \sigma_u \prec_a \sigma_u \) such that \( I(\Pi_{\Sigma_0}(w_{d_2})) = \Pi_{\Sigma_0}(\text{buff}_{d_2}) \) and \( \text{Reach}(\sigma(t', a), \sigma_u \prec_a t') = q_2 \prec_a \sigma_u \). Since \( \sigma_u \prec_a \sigma_u, \sigma_u \prec_a \sigma_u \) after \( \sigma_u \prec_a (\sigma_u, \text{date}(w_{d_2})) \not\in S(\text{buff}_{d_2}) \cup I(\text{buff}_{d_2}) \). Considering the definition of \( I \), \( q_2 \prec_a \sigma_u \not\in w_{d_3}, \) \( \not\in S(\Pi_{\Sigma_0}(\text{obs}(w_{d_3}, \text{date}(w_{d_3})))^{-1}. \text{buff}) \cup I(\Pi_{\Sigma_0}(\text{obs}(w_{d_3}, \text{date}(w_{d_3})))^{-1}. \text{buff}) \), because otherwise \( q_2 \prec_a (\sigma_u, \text{date}(w_{d_3})) \not\in S(\text{buff}_{d_2}) \cup I(\Pi_{\Sigma_0}(\text{obs}(w_{d_3}, \text{date}(w_{d_3})))^{-1}. \text{buff}) \). Moreover, \( I(\Pi_{\Sigma_0}(\text{obs}(w_{d_3}, \text{date}(w_{d_3})))^{-1}. \text{buff}) \) is wrong. In the same way, \( q_2 \prec_a \sigma_u \not\in (w_{d_3}, \text{date}(w_{d_3})) \not\in S(\Pi_{\Sigma_0}(\text{obs}(w_{d_3}, \text{date}(w_{d_3})))^{-1}. \text{buff}) \cup I(\Pi_{\Sigma_0}(\text{obs}(w_{d_3}, \text{date}(w_{d_3})))^{-1}. \text{buff}) \).

Thus, since it is not in \( S \), we can find again a word in \( \mathcal{w}(\Sigma_0) \) s.t. the output of \( E' \) will never be in \( S \) nor \( I \), and end up outside of \( F_c \). Whatever controllable events \( E' \) will output, will never reach \( S \) nor \( I \), and since \( E' \) can only output a limited number of controllable events (no more than \( |\text{buff}| \)), at some point it will not be able to output controllable events anymore, and then there will be an uncontrollable word leading its output outside of \( F_c \). Concatenating all the uncontrollable words obtained from lemma 10, there would be \( \sigma_{d_8} \in \mathcal{w}(\Sigma_0) \) s.t. \( E'(\sigma(t', a), \sigma_{d_8}) \not\in \varphi \).

Thus, if \( a \in \Sigma_0 \), then there exists \( \sigma_u \in \mathcal{w}(\Sigma_0) \) such that \( E'(\sigma(t', a), \sigma_u) \not\in \varphi \).

If \( a \in \Sigma_0 \), then since \( (\sigma, t') \in P(\varphi), a \prec t' \in \text{G(Reach}(\sigma, t'), \Pi_{\Sigma_0}(\text{obs}(\sigma, t'), \sigma)) \). Considering \( q = \text{Reach}(\sigma) \) and \( \text{buff}_{d_2} = \Pi_{\Sigma_0}(\text{obs}(\sigma, t'), \sigma) \), the previous proof (when \( a \in \Sigma_0 \)) still holds. Thus, if \( a \in \Sigma_0 \), there also exists \( \sigma_u \in \mathcal{w}(\Sigma_0) \) s.t. \( E'(\sigma(t', a), \sigma_u) \not\in \varphi \).

This means that whenever \( E'(\sigma) = E_x(\sigma) \land E_x(\sigma(t', a)) \prec_d E'(\sigma(t', a)) \), then there exists \( \sigma_u \in \mathcal{w}(\Sigma_0) \) s.t. \( E'(\sigma(t', a), \sigma_u) \not\in \varphi \). Thus, \( E_x \) is optimal. 

\( \square \)
Proposition 10. The output of $E$ for input $\sigma$ is $E_\sigma(\sigma)$.

Proof. In this proof, we use some notation from Section 4.2:

- $C^E = tw(\Sigma) \times Q \times R_{\geq 0} \times \{\top, \bot\}$ is the set of configurations,
- $c_0^E = (\epsilon, \epsilon, q_0, 0, \bot) \in C^E$ is the initial configuration,
- $T^E = (\langle R_{\geq 0} \times \Sigma \rangle \cup \{\epsilon\}) \times Op \times (\langle R_{\geq 0} \times \Sigma \rangle \cup \{\epsilon\})$ is the alphabet, composed of an optional input, an operation and an optional output,
- The set of operations, to be applied in the given order, is:
  \{compute, dump, pass-uncont, store-cont, delay\}.

Let us also introduce some specific notation. For a sequence of rules $w \in T^E$, we note $input(w) = \Pi_1(w(1)) \Pi_1(w(2)) \ldots \Pi_1(w(|w|))$ the concatenation of all inputs from $w$. In the same way, we define $output(w) = \Pi_1(w'(1)) \Pi_1(w'(2)) \ldots \Pi_1(w'(|w'|))$ the concatenation of all outputs from $w$. Since all configurations are not reachable from $c_0^E$, for a word $w \in T^E$, we will say that $Reach(w) = c$ if $c \leq_{c_0^E} c$, or $Reach(w) = \bot$ if such a $c$ does not exist. Let us also define function $Rules$ which, given a timed word and a date, returns the longest sequence of rules that can be applied with the given word as input at the given date:

$$Rules : \left\{ \begin{array}{l}
tw(\Sigma) \times R_{\geq 0} \rightarrow T^E \\
(\sigma, t) \mapsto \max_E \{w \in T^E \mid input(w) = \sigma \land Reach(w) \neq \bot \land \Pi_1(c) = t\} \end{array} \right.$$  

Since time is not discrete, the rule delay can be applied an infinite number of times by slicing time. Thus, we consider that the rule delay is always applied a minimum number of times, i.e., when two rules delay are consecutive, they are merged into one rule delay, whose parameter is the sum of the parameters of the two rules. The runs obtained are equivalent, but it allows to consider the maximum (for prefix order) of the set used in the definition of Rules. We then extend output to timed words with a date: for $\sigma \in tw(\Sigma)$, and a date $t$, $output(\sigma, t) = output(Rules(\sigma, t))$. For $\sigma \in tw(\Sigma)$ and $t \in R_{\geq 0}$, let $P(\sigma, t)$ be the predicate: "$E_\sigma(\sigma, t) = output(\sigma, t) \land (\langle \sigma_s, \sigma_b, \sigma_c \rangle = store(\sigma)(t, t) \land (\epsilon, \sigma_c') \equiv \epsilon \land \sigma_c = \sigma'_c \land q'_c = Reach(\sigma, t)) \iff \sigma'_c = store(\sigma)(t, t) \land \sigma' = \sigma \land q'_c = Reach(\sigma, t) \land (b = \top \implies G(q'_c, \sigma_c') \neq \emptyset)". Let $P(\sigma)$ be the predicate "$\forall t \in R_{\geq 0}, P(\sigma, t)$ holds". Let us then prove that for all $\sigma \in tw(\Sigma), P(\sigma)$ holds.

Induction basis: For $\sigma = \epsilon$, let us consider $t \in R_{\geq 0}$. Then, $store(\epsilon, t) = (\epsilon, \epsilon, \epsilon)$, and $Reach(\epsilon, t) = (l_0, v_0 + t)$. On the other hand, the only rules that can be applied are delay, and possibly compute, since there is no input, nor any element to dump. Thus, $Rules(\epsilon, t) = \epsilon / delay(t)/\epsilon$, or there exists $t' \geq t$ s.t. $Rules(\epsilon, t) = \epsilon / delay(t')/\epsilon$. $\epsilon / compute(t)/\epsilon / delay(t - t')/\epsilon$. Let us consider $c = Reach(\epsilon, t)$, then $c = (\epsilon, \epsilon, \epsilon, l_0, v_0 + t, t, \emptyset)$. If rule compute appears in $Rules(\epsilon, t)$, then $b = \top$, meaning that $G(q_0 \epsilon/\epsilon, c, \epsilon) \neq \emptyset$, and thus that $G(q_0 \epsilon/\epsilon, c, \epsilon) \neq \emptyset$ since $t \geq t'$. Otherwise $b = \bot$. All the other values remain unchanged between the two cases. In both cases, $output(Rules(\epsilon, t)) = \epsilon = E_\epsilon(\epsilon, t)$. Thus, $P(\epsilon)$ holds.

Induction step: Let us suppose now that for some $\sigma \in tw(\Sigma), P(\sigma)$ holds. Let us consider $(t', a) \in R_{\geq 0} \times \Sigma$, s.t. $(\sigma(t', a)) \in tw(\Sigma)$. Let us then prove that $P(\sigma, (t', a))$ holds. Let us consider $t \in R_{\geq 0}$, $c = (\langle \sigma'_c, \sigma_c', q'_c, t' \rangle, b) = Reach(\sigma, (t', a)), (\sigma_s, \sigma_b, \sigma_c) = store(\sigma, (t', a)), \sigma = store(q)(\sigma, (t', a), t)$, $q'_c = q_c = Reach(\sigma, (t', a), t)$, and $P(\sigma, (t', a), t)$ trivially holds, since $P(\sigma)$ holds. Thus, in the following, we consider that $t \geq t'$, so that $store(q)(\sigma, (t', a), t, t) = store(q)(\sigma, (t', a), t)$.

If $a \in \Sigma_a$, rule pass-uncont can be applied. Let us consider $c' = c$ after $(t', a)/pass-uncont((t', a))(t', a))$. Then, $c' = (\epsilon, \Pi_2(\sigma'_c), \sigma'_c, q'_c, t', \bot)$, with $q'_c = q_c'$ after $(0, a)$. Then, if $t \geq t'_f$, where $t'_f = \min(t', t'\lfloor 0, t' \geq t \land G(q'_c, (t', t' - t'), \Pi_2(\sigma'_c), \sigma'_c) \neq \emptyset)$, then rule delay $(t'_f - t')$ can be applied, followed by rule compute. Since $q'_c = Reach(\sigma, (t', a), t', \top)$, $\sigma'_c = nobs(\sigma, t')$, and $\sigma'_c = \sigma_c$ by in-
duction hypothesis), then \( G(q') after (e, t''-t')) = G(Reach(\sigma_e, (t', a), t')) \), \( \Pi_{\Sigma}(\sigma_e^\bot) \), \( \sigma_e \), thus \( t_y^2 = t_1 \), where \( t_1 \) is defined in Definition 16. Thus, \( c' after (\epsilon/delay (t_y^2 - t'))/\epsilon \).

(\epsilon/compute /\epsilon) = \( \langle \sigma_e^\bot, \sigma_e^\bot, q' after (e, t_1-t'), t_1, T \rangle \), with \( \sigma_e^\bot = \kappa_e(q after (e, t_1-t'), \Pi_{\Sigma}(\sigma_e^\bot), \sigma_e) \) + \( t_1 = \kappa_e(Reach(\sigma_e, (t', a), t_1), \Pi_{\Sigma}(\sigma_e, \sigma_e)) + \) \( t_1 = \sigma_e \), and thus \( \sigma_e^\bot = \sigma_e \). Then, rules delay and dump can be applied until date \( t \) is reached. In the end, \( \text{Reach}(\text{Rules}(\sigma(t', a), t)) = c' after w, \)

where \( w \) is composed of an alternation of rules delay and dump, thus \( \text{Reach}(\text{Rules}(\sigma(t', a), t)) = \langle \text{obs}(\sigma_e^\bot, t), \sigma_e^\bot, q' after (\text{obs}(\sigma_e^\bot, t) - (t', t-t'), t, T) = \langle \text{obs}(\sigma_e, t), \sigma_e, \text{Reach}(\sigma_e, t), t, T \rangle \).

Then, \( \text{output}(\text{Rules}(\sigma(t', a), t)) = \text{output}(\text{Rules}(\sigma(t', a), t)) = \text{output}(\text{Rules}(\sigma(t', a), t)) \).

Thus, if \( t \geq t_1 \), \( \text{P}(\sigma(t', a), t) \) holds. Otherwise, \( t < t_1 \), and then rule dump cannot be applied, since \( \Pi_{\Sigma}(\epsilon') = \bot \), and rule compute also cannot be applied. Thus, the only rule that can be applied is delay, so that \( \text{Reach}(\text{Rules}(\sigma(t', a), t)) = \langle \epsilon, \Pi_{\Sigma}(\sigma_e^\bot), \sigma_e^\bot, q' after (\epsilon, t-t'), t', 1 \rangle \).

Since \( t < t_1 \), this means that \( \sigma_d = \epsilon \), and \( \sigma_e = \Pi_{\Sigma}(\sigma_e) \). \( \sigma_e \). Thus, \( \text{output}(\text{Rules}(\sigma(t', a), t)) = \text{output}(\text{Rules}(\sigma(t', a), t)) \).

- Otherwise, \( a \in \Sigma \). Then, rule store-cont can be applied. Let us consider \( c' = c after ((t', a)/\text{store-cont}(a)/\epsilon) \). Let us consider \( t_y^2 = \min(\{t'' \in \mathbb{R}_{\geq 0} \mid t'' \geq t' \wedge G(q'' after (e, t''-t'), \Pi_{\Sigma}(\sigma_e^\bot), \sigma_e) \neq \emptyset\}) \). Since \( G(q'' after (e, t''-t'), \Pi_{\Sigma}(\sigma_e^\bot), \sigma_e) = G(\text{Reach}(\sigma_e, t''), \Pi_{\Sigma}((\\text{obs}(\sigma_e, t''))/\sigma_e, a)) \), it follows that \( t_y^2 = t_2 \) as defined in Definition 16. If \( t \geq t_y^2 = t_2 \), then rule delay/(t_2-t') can be applied, followed by rule compute. Then, \( c' after ((\epsilon/delay (t_2-t')/\epsilon)/\text{compute}(t_2-\epsilon)) = \langle \sigma_e^\bot, \sigma_e^\bot, q after (e, t_2-t'), t_2, T \rangle \), where \( \sigma_e^\bot = \kappa_e(q after (e, t_2-t'), \Pi_{\Sigma}(\sigma_e^\bot), \sigma_e) + \) \( t_2 = \kappa_e(Reach(\sigma_e, t_2), \Pi_{\Sigma}(\sigma_e, \sigma_e)) + \) \( t_2 = \sigma_e \). Then, \( \sigma_e^\bot = \sigma_e \). Then, an alternation of rules delay and dump can be applied until date \( t \) is reached. This leads to \( \text{Reach}(\text{Rules}(\sigma(t', a), t)) = \langle \text{obs}(\sigma_e^\bot, t), \sigma_e^\bot, q after (\text{obs}(\sigma_e^\bot, t), t, T) = \langle \text{obs}(\sigma_e, t), \sigma_e, \text{Reach}(\sigma_e, t), t, T \rangle \). Moreover, \( \text{output}(\text{Rules}(\sigma(t', a), t)) = \text{output}(\sigma(t', a), t, a) = \sigma_e \).

Thus, if \( t \geq t_2 \), \( \text{P}(\sigma(t', a), t) \) holds. Otherwise, \( t < t_2 \), meaning that \( \sigma_e^\bot = \epsilon = \sigma_d \), and \( \sigma_e^\bot = \Pi_{\Sigma}(\sigma_e^\bot), \sigma_e^\bot, a = \Pi_{\Sigma}((\\text{obs}(\sigma_e, t'))/\sigma_e, a = \sigma_e, and\text{output}(\sigma(t', a), t) = \text{output}(\sigma(t', a) = \sigma_e = \text{E}_e(\sigma(t', a), t) \). Thus, \( \text{P}(\sigma(t', a), t) \) holds.

Thus, by induction, for all \( \sigma \in tw(\Sigma) \), \( \text{P}(\sigma) \) holds. In particular, for all \( \sigma \in tw(\Sigma) \), and for all \( t \in \mathbb{R}_{\geq 0} \), \( \text{output}(\sigma, t) = \text{E}_e(\sigma, t) \), meaning that the output of the enforcement monitor \( E \) with input \( \sigma \) at time \( t \) is exactly the output of function \( E_e \) with the same input and the same date.