Runtime Enforcement Using Büchi Games
Matthieu Renard, Antoine Rollet, Yliès Falcone

To cite this version:
Matthieu Renard, Antoine Rollet, Yliès Falcone. Runtime Enforcement Using Büchi Games. ACM. Model Checking Software - 24rd International Symposium, SPIN 2017, Co-located with ISSTA 2017, Jul 2017, Santa Barbara, United States. <hal-01509827v3>

HAL Id: hal-01509827
https://hal.archives-ouvertes.fr/hal-01509827v3
Submitted on 17 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.
Runtime Enforcement Using Büchi Games

Matthieu Renard  
LaBRI  
Bordeaux INP  
University of Bordeaux  
Bordeaux, France  
matthieu.renard@labri.fr

Antoine Rollet  
LaBRI  
Bordeaux INP  
University of Bordeaux  
Bordeaux, France  
antoine.rollet@labri.fr

Yliès Falcone  
Univ. Grenoble Alpes, Inria  
Laboratoire d’Informatique de Grenoble  
F-38000, Grenoble, France  
ylies.falcone@univ-grenoble-alpes.fr

ABSTRACT
We leverage Büchi games for the runtime enforcement of regular properties with uncontrollable events. Runtime enforcement consists in modifying the execution of a running system to have it satisfy a given regular property, modelled by an automaton. We revisit runtime enforcement with uncontrollable events and propose a framework where we model the runtime enforcement problem as a Büchi game and synthesise sound, compliant, and optimal enforcement mechanisms as strategies. We present algorithms and a tool implementing enforcement mechanisms. We reduce the complexity of the computations performed by enforcement mechanisms at runtime by pre-computing the decisions of enforcement mechanisms ahead of time.

KEYWORDS
Runtime Verification, Runtime Enforcement, Games, Automata

1 INTRODUCTION
Runtime Verification (RV) consists in checking if the execution of a running system satisfies some given specification. Unlike static verification, RV studies a real execution of a system, possibly after deployment. This paper deals with runtime enforcement, an extension of runtime verification where executions are corrected when they violate the property [1, 10, 11, 15]; see [7] for a tutorial on runtime enforcement. The considered properties are regular properties, that are represented by deterministic and complete automata. All such properties are monitorable since they are defined with a semantics over finite words [8]. An enforcement mechanism modifies an execution: it takes an execution as input and outputs a possibly-different execution. Enforcement mechanisms may operate online, meaning that they modify the executions of a system while it is running, or offline, by reading a log of system events. While working online, enforcement mechanisms can add a time overhead due to their need to compute a correct output. We distinguish two categories of events: controllable events that can be modified by an enforcement mechanism, and uncontrollable events that can only be observed by the enforcement mechanism. Enforcement mechanisms should be sound and compliant, meaning that the output should satisfy the specification when it is possible, and that the output should be as close to the input as possible, respectively. The general scheme is given in Fig. 1.

Motivations. In this paper, we improve the modelling of the enforcement mechanisms proposed in [13, 14], as well as the computation of their output. Such mechanisms should impact the system as little as possible, thus reducing the time spent by enforcement mechanisms to compute their behaviour allows us to use them in a more realistic way. For example, in interactive systems, the system interacts with a human user, if an event takes too long to be output, the user may think that the system failed. It could also be useful for embedded systems, where computing power may be reduced. Computing the behaviour of the enforcement mechanism ahead of the execution and storing it ensures that the computation does not depend on the size of the automaton, thus allowing the time spent on online computations by enforcement mechanisms to be reduced and more predictable. Indeed, not exploring the whole execution tree for all possible outputs at runtime, as a naive approach would do, allows us to have computation times that vary less (with a naive approach, the computation time can become very important with an increasing number of stored controllable events).

Challenges. Storing the behaviour of enforcement mechanisms to improve their online computation time induces some changes compared to previous work (as [13, 14]). The main difficulty resides in the fact that the number of states of the enforcement mechanism is infinite. Indeed, the mechanism has the possibility to store uncontrollable events that it may choose to release or not. The number of events that can be stored at the same time is not bounded, thus the number of states of the enforcement mechanism is infinite. Therefore, computing and storing its behaviour for all possible input traces entails defining appropriate abstractions.

Contributions. A first approach of enforcement with uncontrollable events has been presented in [14] providing sound and compliant enforcement mechanisms. An optimal version of this approach may be found in [13]. In this paper, we propose to extend this work by computing the behaviour of the enforcement mechanism using Büchi games. Using Büchi games allows us to compute the behaviour of the enforcement mechanism before the execution, thus allowing to trade time complexity with space complexity. When

Figure 1: Schematic description of an enforcement mechanism $E$, modifying the execution $\sigma$ of the system $S$ to $E(\sigma)$, so that it satisfies the property $\varphi$. 

Conference'17.
© .
using an online enforcement mechanism (i.e. an enforcement mechanism on a running system), it allows us to produce the output faster in the worst case than in [14] and [13] where the behaviour of the enforcement mechanism was computed every time an event was received. Leveraging games, when an event is received, the enforcement mechanism only follows a path in a graph, and the destination vertex is sufficient to indicate if a stored event should be output or not. Moreover, the generated graph can be visualised to understand the behaviour of the enforcement mechanism, and it also shows clearly when an enforcement mechanism can effectively ensure soundness. We redefine soundness, compliance and optimality using a set-theoretic view of the system, thus providing a global vision of the system based on inputs and outputs at any instant. We give the algorithms (and their complexity analysis) implementing the behaviour of enforcement mechanisms. We finally present a tool implementing the proposed approach.

2 PRELIMINARIES AND NOTATION

General notions. An alphabet is a finite set of symbols. A word over an alphabet Σ is a sequence over Σ. The set of finite words over Σ is denoted Σ*. The length of a finite word w is noted |w|, and the empty word is noted ε. Σ+ stands for Σ* \ {ε}. A language over Σ is any subset L ⊆ Σ*. The concatenation of two words w and w' is noted w.w' (or w∥w' when clear from the context). A word w' is a prefix of a word w, noted w' ≦ w, if there exists a word w'' such that w = w''w'. Word w'' is called the residual of w after reading the prefix w', noted w'' = w'(w''w = w). Note that w'.w'' = w''−1.w. These definitions are extended to languages in the natural way. A language L ⊆ Σ* is extension-closed if for any words w ∈ L and w' ∈ Σ* such that |w| ≤ |w'|, we have w.w' ∈ L.

It is known that it is possible to compute the set Σ of times the set V is visited an infinite number of times (Balbiani games). Thus, given a subset V of V, it is possible to play a two-player game in the arena A = (V0, V1, E). A play over A is a path in G, i.e. a sequence of vertices such that there exists an edge in G between any two consecutive vertices in the sequence. A strategy for player P0 is a mapping σ : V ∗ → V such that for all π ∈ V ∗, for all v0 ∈ V0, (v0, σ(π.v0)) ∈ E, i.e. the strategy gives a vertex that can be reached from v0. Note that V0 is thus the set of vertices from which P0 can play, whereas the other player, P1, plays from the vertices in V1. Strategies for P1 are defined in a similar way, replacing v0 by V1. A play π = v0, v1, ... is consistent with the strategy σ if for any v0 ∈ V0, v1+1 = σ(v0, v0, ..., v0), meaning that the strategy was followed for any vertex in V0. The goal of a game can be, for example, to reach a state in a given subset of V (reachability game), or to ensure that a given subset of V is visited an infinite number of times (Büchi games). Thus, given a subset F ∈ Σ ⊆ V of vertices, the Büchi game (A, F) for P0 consists in finding a winning strategy σ such that all plays π over A consistent with σ visit an infinite number of times the set F (i.e. if π is consistent with σ, π ∈ (V ∗.F)ω). It is known that it is possible to compute the set V0 of winning vertices for P0 (i.e. the set of vertices from where there exists a winning strategy for P0), and the associated winning strategy from all these vertices. From all the other vertices (in V \ V0), there exists a winning strategy for P1, i.e. W1 = V \ V0, thus P0 can not win the game if P1 plays perfectly from one of these vertices.

Figure 2: Property φex modelling writes on a shared storage device

represented by a deterministic and complete automaton AR. Given a complete and deterministic automaton A = (Q, q0, Σ, ↦, F) and a word σ ∈ Σ∗, for q ∈ Q, we note q after σ the only state such that q → (q after σ). The completeness of A ensures that q after σ exists, and its determinism ensures that it is unique. We also note Reach(σ) = q0 after σ. We extend these definitions to languages: if L is a language, q after L = ∪q∈L q after σ and Reach(L) = q0 after L.

Graphs and Büchi games. A graph is a couple (V, E) such that V is a set of elements called vertices, E ⊆ V × V is a relation defining edges between the vertices. Given a graph G = (V, E) and a partition of V into two subsets V0 and V1, it is possible to play a two-player game in the arena A = (V0, V1, E). A play over A is a path in G, i.e. a sequence of vertices such that there exists an edge in G between any two consecutive vertices in the sequence. A strategy for player P0 is a mapping σ : V ∗ → V such that for all π ∈ V ∗, for all v0 ∈ V0, (v0, σ(π.v0)) ∈ E, i.e. the strategy gives a vertex that can be reached from v0. Note that V0 is thus the set of vertices from which P0 can play, whereas the other player, P1, plays from the vertices in V1. Strategies for P1 are defined in a similar way, replacing v0 by V1. A play π = v0, v1, ... is consistent with the strategy σ if for any v0 ∈ V0, v1+1 = σ(v0, v0, ..., v0), meaning that the strategy was followed for any vertex in V0. The goal of a game can be, for example, to reach a state in a given subset of V (reachability game), or to ensure that a given subset of V is visited an infinite number of times (Büchi games). Thus, given a subset F ⊆ V of vertices, the Büchi game (A, F) for P0 consists in finding a winning strategy σ such that all plays π over A consistent with σ visit an infinite number of times the set F (i.e. if π is consistent with σ, π ∈ (V ∗.F)ω). It is known that it is possible to compute the set V0 of winning vertices for P0 (i.e. the set of vertices from where there exists a winning strategy for P0), and the associated winning strategy from all these vertices. From all the other vertices (in V \ V0), there exists a winning strategy for P1, i.e. W1 = V \ V0, thus P0 can not win the game if P1 plays perfectly from one of these vertices.

3 ENFORCEMENT MONITORING OF PROPERTIES USING BÜCHI GAMES

This paper revisits and extends the approach described in [14] by writing the definitions in a set-theoretic view instead of a functional
way and proposing a new synthesis technique of Enforcement Mechanisms (EM) using Büchi games.

In this section, \( \varphi \) is a regular property defined by a complete and deterministic automaton \( \mathcal{A}_\varphi = (Q, q_0, \Sigma, \rightarrow, F) \). Recall that the general scheme of an 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, 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).\(^2\) Thus, an EM may interleave controllable and uncontrollable events.

### 3.1 Enforcement Functions and their Requirements

We consider an alphabet of actions \( \Sigma \). We consider functions as sets: a function from a set \( A \) to a set \( B \) is a set \( f \subseteq A \times B \) such that for any element \( a \in A \), there is a unique \( b \in B \) such that \( (a, b) \in f \). We note \( \mathcal{F}(A, B) \) the set of all functions from \( A \) to \( B \). An enforcement function is a description of the input/output behaviour of an EM. It is a function from \( \Sigma^* \) to \( \Sigma^* \), increasing on \( \Sigma^* \) (with respect to \( \preceq \)):

**Definition 3.1 (Enforcement function).** A function \( f \in \mathcal{F}(\Sigma^*, \Sigma^*) \) is an enforcement function if \( \forall i_1 \in \Sigma^*, \forall i_2 \in \Sigma^*(, (i_1 \preceq i_2 \land (i_1, o_1) \in f \land (i_2, o_2) \in f) \implies o_1 \preceq o_2) \). We note \( \mathcal{F}_{\text{emf}} \) the set of all enforcement functions.

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, the usual purpose of an EM is to ensure that the executions of a running system satisfy a property, thus its enforcement function has to be sound, meaning that its output always satisfies the property:

**Definition 3.2 (Soundness).** An enforcement function \( E \in \mathcal{F}_{\text{emf}} \) is sound with respect to \( \varphi \) in an extension-closed set \( S \subseteq \Sigma^* \) if \( \forall i \in S, (i, o) \in E \implies o \models \varphi \). We note \( \mathcal{F}_{\text{snd}}(S) \) the set of all enforcement functions that are sound in \( S \).

The reception of 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. Thus, the enforcement mechanism would not be able to make the property satisfied. Consequently, in Definition 3.2, soundness is not defined for all words in \( \Sigma^* \), but in a subset \( S \), since the property could not be enforceable from the initial state. In practice, \( S \) needs to be extension-closed to ensure that once the enforcement mechanism becomes sound, its output will always satisfy the property afterwards.

The usual notion of transparency in enforcement monitoring (cf. [11, 15]) states that the output of an enforcement function is the longest prefix of the input satisfying the property, implying 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 cannot be ensured, and we define the weaker notion of compliance.

**Definition 3.3 (Compliance).** \( E \in \mathcal{F}_{\text{emf}} \) is compliant with respect to \( \Sigma_u \) and \( \Sigma_c \), noted compliant\( \left( E, \Sigma_u, \Sigma_c \right) \), if \( \forall i \in \Sigma^*, (i, o) \in E \implies (o \preceq \sigma \land o \models \varphi \land o_u \in \Sigma_u, ((i, a, o') \in E \implies o_u \preceq o')) \). We note \( \mathcal{F}_{\text{cl}}(\Sigma_u, \Sigma_c) \) the set of all enforcement functions that are compliant with respect to \( \Sigma_u \) and \( \Sigma_c \).

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. When clear from the context, the partition is not mentioned: \( E \) is said to be compliant, we note it compliant\( (E) \), and the set of all compliant functions is then denoted \( \mathcal{F}_{\text{cl}} \).

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. We define the optimality of sound and compliant enforcement functions as follows:

**Definition 3.4 (Optimality).** An enforcement function \( E \in \mathcal{F}_{\text{snd}}(S) \cap \mathcal{F}_{\text{cl}}(\Sigma_u, \Sigma_c) \) is optimal in \( S \) if:

\[
\forall E' \in \mathcal{F}_{\text{ snd}}(S) \cap \mathcal{F}_{\text{ cl}}(\Sigma_u, \Sigma_c), \forall i \in S, \forall o_u \in \Sigma, ((i, a, o) \in E \land (i, a, o') \in E') \implies p' \preceq o'.
\]

Intuitively, optimality states that outputting a longer word than an optimal enforcement function breaks soundness or compliance.

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 in the definition of soundness (see Definition 3.2).

**Example 3.5.** We consider a simple 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 \( \varphi_{ex} \) (see Fig. 2) formalises the above requirement. \( \varphi_{ex} \) is not enforceable if the uncontrollable alphabet is \( \{\text{LockOn, LockOff, Auth}\} \) 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 prevent \( \varphi_{ex} \) from being enforced 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 3.5 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 is then possible to define a subset of \( \Sigma^* \) in which an enforcement function is sound.

Footnotes:

1. This notion of uncontrollable event should not be confused with the notion of uncontrollable transition used in some game theory (e.g. [4]).
2. 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.

3. Uncontrollable events are emphasised in italics.
A compliant enforcement mechanism may store the received controllable events to emit them after having received another event, possibly uncontrollable. To ensure soundness, the enforcement mechanism must know if it is possible to emit some of its stored controllable events in order to reach an accepting state, from which it will be able to reach an accepting state even if some uncontrollable events are received later on. Thus, it should compute the set of words it can emit to reach such an accepting state. This set will be called $G$, and to define it, we solve a Büchi game over a graph representing the possible actions of an enforcement monitor. Solving a Büchi game over a graph with a set of goal nodes (referred to as Büchi nodes) consists in finding the nodes of the graph from where it is possible to reach a Büchi node infinitely often, no matter what the opponent’s strategy is. Note that a winning node of a Büchi game is also a winning node for the reachability game on the same graph, with the vertices of the graph are composed of a state in $Q$, uncontrollable and controllable events of the enforcement mechanism. There exists two of each. Thus, the enforcement mechanism can emit all the events it wins the Büchi game, over this graph. To overcome this, the graph is reduced to a graph with a finite number of vertices. To do this, first note that the number of vertices is infinite because the set $\Sigma_c^w$ is not bounded. Thus, $\Sigma_c^w$ must be abstracted to a finite set. Since the goal is to reach a state in $F$, the stored controllable events are used to reach some states in $Q$. Since $Q$ is finite, more controllable events than $|Q|$ means that (following the Pumping lemma) there is a loop, i.e. some state in $Q$ is reached twice when emitting all the controllable events. Thus, the enforcement mechanism can emit all the events until it reaches this state for the second time, and then its decision will only depend on the remaining controllable events. Thus, the number of controllable events can be reduced to at most $|Q|$. More precisely, we can reduce $\Sigma_c^w$ to the set of words that allow to reach a new state (i.e. a state that is not reached by one of its prefixes) from at least one state in $Q$. Let us call this set $\Sigma_c^n$, and define it as follows:

$$\Sigma_c^n = \{ w \in \Sigma_c^w \mid \exists q \in Q, \exists c \in \Sigma_c, \forall w' \leq w, q after w.c \neq q after w'\}$$

As explained previously, since $Q$ is finite, $\Sigma_c^n$ is finite as well. Now, let us redefine $G$ to an abstraction of the game graph:

$$G = (V', E'),$$

where $V' = Q \times \Sigma_c^n \times \{0, 1\}$, and $E'$ is the same set as $E$, but considering vertices in $V'$ instead of $V$.

$G$ then has a finite number of vertices. Let us now consider $W_0 \subseteq V$ the set of vertices that are winning for $P_0$ in the Büchi game over $G$, with the set of Büchi (accepting) vertices being $F \times \Sigma_c^n \times \{0, 1\}$.

**Example 3.8.** The graph in Fig. 3 is computed from property $p_{ex}$, with $\textsf{Write}$ abbreviated $w$ in the second member of the nodes. The Büchi nodes are double circled, and the winning nodes for player 0 (i.e. nodes in $W_0$) are in blue and rounded rectangles (in our example, all the Büchi nodes are winning). Each edge has a different colour and a different head depending on the set it belongs to. Blue edges (empty triangular head) belong to $E_1$, green edges (filled triangular head) belong to $E_2$, orange edges (empty diamond head) belong to $E_4$, and red edges (filled diamond head) belong to $E_3 \cup E_5$. Each edge is represented only once, even if there are multiple edges in the set (for example, because multiple uncontrollable events lead to the same state from one state). The squared vertex is the initial vertex, and “~” stands for “$e$” (empty buffer).

Since the initial vertex is black (not rounded), this means that it is impossible to ensure that the property will be satisfied from the beginning. The only way to reach a winning state is to follow a red edge from a vertex in $[q_1] \times \{e, w, w.e\} \times \{0\}$, that corresponds to being uncontrollable event $\textsf{Auth}$ (since it leads to a state in $[q_2] \times \{e, w, w.e\} \times \{0\}$). Then, $\textsf{Write}$ events can only be emitted when in state $q_1$. This behaviour is the one expected, since in $p_{ex}$, the only way to reach a state in $F$ from $q_0$ is to follow a path labelled by $\textsf{Auth}$ reaching $q_1$. Then, from $q_1$, it is possible to emit $\textsf{Write}$ events, and if some uncontrollable events are received that lead to...
Definition 3.9 (G). For a state $q \in Q$ and a word of controllable events $\sigma \in \Sigma_\sigma$, we define the set $G(q, \sigma)$ as follows:

$$G(q, \sigma) = \{ w \in \Sigma^* \mid w \preceq \sigma \land q \text{ after } w \in F \land (q \text{ after } w, \max_{<w}((w' \preceq w^{-1} \sigma \mid w' \in \Sigma^+_c)), 1) \in W_0 \}.$$ 

Intuitively, $G$ is the set of words that can be output by a compliant enforcement mechanism to ensure soundness.

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

Definition 3.10 (Functions $store_\phi$, $E_\phi$). Function $store_\phi \in \Sigma^* \times (\Sigma^* \times \Sigma^+_c)$ is defined by induction on its first member as follows:

- $(\epsilon, (\epsilon, \epsilon)) \in store_\phi$;
- for $\sigma \in \Sigma^*$ and $a \in \Sigma$, let $(\sigma, (\sigma_a, \sigma_c)) \in store_\phi$, then:

$$\begin{cases} (\sigma.a, (\sigma_a, a, \sigma_c')) \in store_\phi & \text{if } a \in \Sigma_a, \\
(\sigma.a, (\sigma_a, \sigma_c', \sigma_c'')) \in store_\phi & \text{if } a \in \Sigma_c, \\
\end{cases}$$

where:

$$\kappa_\phi(q, w) = \max_q(G(q, w) \cup \{e\}),$$

for $q \in Q$ and $w \in \Sigma^+_c$,

$$\sigma_a' = \kappa_\phi(\text{Reach}(\sigma_a, \sigma_c)), \quad \sigma_c' = \sigma_a'^{-1} \sigma_c,
\sigma_a'' = \kappa_\phi(\text{Reach}(\sigma_a), (\sigma_c', \sigma_c), a), \quad \sigma_c'' = \sigma_a''^{-1} \sigma_c.$$

The enforcement function $E_\phi \in T_{\text{enf}}$ is defined as:

$$E_\phi = \{(\sigma, \sigma') \mid \exists w \in \Sigma^+_c, (\sigma, (\sigma', w)) \in store_\phi\}.$$

Figure 4: Enforcement function

Figure 4 gives a scheme of the behaviour of the enforcement function. Intuitively, $\sigma_a$ is the word that can be released as output, whereas $\sigma_c$ 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 (i.e. they lead to a vertex in $W_1 = V \setminus W_0$). Upon receiving a new event $a$, the enforcement mechanism distinguishes two cases:

- If $a$ belongs to $\Sigma_a$, then it is output, as required by compliance. Then, the longest prefix of $\sigma_c$ that satisfies $\varphi$ and leads to a vertex in $W_0$ is also output.
- If $a$ is in $\Sigma_c$, then it is added to $\sigma_c$, and the longest prefix of this new buffer that satisfies $\varphi$ and leads to a vertex in $W_0$ is emitted, if it exists.

In both cases, $\kappa_\phi$ 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 $\epsilon$ if this set is empty. The parameters of $\kappa_\phi$ 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.

Some properties are not enforceable (see Example 3.5), 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 $E_\phi$ is sound in $\text{Pre}(\varphi)$, as stated in Proposition 3.14:

$\ast E_\phi$ and $store_\phi$ depend on $\Sigma_a$ and $\Sigma_c$, but we did not write it in order to lighten the notations.
Definition 3.11 (Pre). The set of input words Pre(φ) ⊆ Σ* is defined as follows:

Pre(φ) = {σ ∈ Σ* | G(Reach(σw_P, σw_Q) ≠ ∅), Σ_P}

Intuitively, Pre(φ) is the set of words in which E_φ is sound. This set is extension-closed, as required by Definition 3.2. In E_φ, using W_φ ensures that once the set G is not empty, it will never be afterwards, no matter what messages are received. Thus, Pre(φ) is the set of input words such that the output of E_φ belongs to G. Since E_φ outputs only uncontrollable events until G becomes non-empty, the definition of Pre(φ) considers that the state reached is the one that is reached by emitting only the uncontrollable events of σ, and the corresponding buffer would then be the controllable events of σ.

Example 3.12. Considering the property φ_ex as shown in Fig. 2, with the uncontrollable alphabet Σ_u = [Auth, LockOff, LockOn], Pre(φ_ex) = Write'.Auth.Σ_B. Indeed, from the initial state q_0, if an uncontrollable event, say LockOff, is received, then q_3 is reached, which is a non-accepting sink state, and thus any vertex in (q_3) × Σ_u × {0, 1} will not be in W_φ. In order to reach a vertex in W_φ (i.e. a vertex in (q_3) × Σ_u × {0, 1}, it is necessary to read Auth. Once Auth is read, q_4 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 Write events when in q_2 until a LockOff event is received. Consequently, (q_1, q_2) × Σ_u × {0, 1} ⊆ W_φ, and thus Pre(φ_ex) = Write'.Auth.Σ_B, since Write events can be buffered while in state q_0 until event Auth is received, leading to a vertex in (q_1) × (Write' ∩ Σ_u) × {0, 1} ⊆ W_φ.

Table 1: Evolution of (σ, (σ_a, σ_c)) ∈ store_φ

<table>
<thead>
<tr>
<th>σ_a</th>
<th>σ</th>
<th>σ_c</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth</td>
<td>ε</td>
<td>ε</td>
</tr>
<tr>
<td>Auth.LockOn</td>
<td>Auth</td>
<td>ε</td>
</tr>
<tr>
<td>Auth.LockOn.Write</td>
<td>Auth.LockOn</td>
<td>ε</td>
</tr>
</tbody>
</table>

E_φ (as per Definition 3.10) is an enforcement function that is sound with respect to φ in Pre(φ), compliant with respect to Σ_u and Σ_c, and optimal in Pre(φ).

Proposition 3.13. E_φ is an enforcement function as per Definition 3.1.

Sketch of proof: We have to show that for all σ and σ′ in Σ*, (σ, σ_o) ∈ E_φ ∧ (σ, σ_o) ∈ E_φ ⇒ σ_o = σ_o'. Following the definition of store_φ, this holds provided that σ′ ∈ Σ (i.e. σ′ is a word of size 1). Since = is an order, it follows that the proposition holds for all σ′ ∈ Σ*.

Proposition 3.14. E_φ is sound with respect to φ in Pre(φ), as per Definition 3.2.
state, but since the vertex is not in $W_0$, there would exist again an uncontrollable word leading to a non-accepting state and a vertex not in $W_0$. 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 $E_\phi$ is optimal in $\text{Pre}(\phi)$, since it outputs the longest word that allows us to be both sound and compliant.

### 3.3 Enforcement Monitors

Enforcement monitors are operational descriptions of enforcement mechanisms. We give a representation of an enforcement mechanism for a property $\phi$ as an input/output transition system. The input/output behaviour of the enforcement monitor is the same as the one of the enforcement function $E_\phi$ defined in Section 3.2. Enforcement monitors are purposes to ease the implementation of enforcement mechanisms, since they give an operational representation of the enforcement mechanism.

**Definition 3.17 (Enforcement monitor).** An enforcement monitor $E$ for $\phi$ is a transition system $(C^E, e^E, \Gamma^E, \cdot)$ such that:

- $C^E = Q \times \Sigma^*$ is the set of configurations.
- $e^E = \langle q_0, e \rangle$ 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.
- $\cdot: C^E \subseteq C^E \times \Gamma^E \times C^E$ is the transition relation, defined as the smallest relation obtained by applying the following rules in order (where $w / \Rightarrow / w'$ stands for $(w, \Rightarrow, w') \in \Gamma^E$):
  - **DUMP:** $\langle q, a.c_\sigma \rangle \xrightarrow{\text{dump}(a)/a} \langle q', c_\sigma \rangle$, if $a \in \Sigma_c$, $G(q, a.c_\sigma) \neq \emptyset$ and $G(q, a.c_\sigma') \neq \emptyset$, with $q' = q$ after $a$.
  - **PASS-UNCONT:** $\langle q, c_\sigma \rangle \xrightarrow{a/\text{pass-uncont}(a)/a} \langle q', c_\sigma \rangle$, with $a \in \Sigma_a$ and $q' = q$ after $a$.
  - **STORE-CONT:** $\langle q, c_\sigma \rangle \xrightarrow{a/\text{store-cont}(a)/e} \langle q, c_{\sigma.a}, a \rangle$, 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 $\mathcal{A}_\phi$ with the output of the monitor. The word of controllable events $\sigma$ 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 $c_\sigma$ in the definition of $store_\phi$, whereas $c_\sigma$ is here represented by state $q$ which is the first member of the configuration, such that $q = \text{Reach}(c_\sigma)$.

**Proposition 3.18.** The output of the enforcement monitor $E$ for input $\sigma \in E_\phi(\sigma)$.

In Proposition 3.18, the output of the enforcement monitor is the concatenation of all the outputs of the word labelling the path followed when reading $\sigma$.

**Sketch of proof.** The proof is made by induction on the input $\sigma \in \Sigma^*$. We just consider the rules that can be applied when receiving a new event. If the event is controllable, then rule store-cont() can be applied, possibly followed by rule dump() applied once or more times. If the event is uncontrollable, then rule pass-uncont() can be applied, again possibly followed by rule dump() applied once or more 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 $G$. Thus, the output of all the applications of the rule dump() corresponds to the computation of $k_\phi$ in the definition of $store_\phi$, and consequently the outputs of $E$ and $E_\phi$ are the same.

## 4 Algorithms and Implementation

We describe some of the algorithms that allow us to use a game graph (as per Definition 3.6) to define an enforcement mechanism, and discuss their time complexity. We suppose that the set of winning nodes of the graph is known, as there exist well-known algorithms to compute it (see for example [5]).

### 4.1 Algorithms

Algorithm 1 computes the set $\Sigma_c^n$ (see Section 3.2), the set of words that allow to reach a state that is unreachable with all its prefixes from at least one state. Algorithm 1 uses a recursive function described in Algorithm 2. The algorithm builds the words incrementally, adding each possible event to a word in the set, until adding an event does not allow to reach a new state from any state. We make use of arrays of one and two dimensions. Function arrayInit($m$, $n$) returns an array of $m$ rows and $n$ columns, when $n$ is not specified, it returns a 1-dimensional array of size $m$. The returned array is filled with 0.

```
input : An automaton $\mathcal{A} = (Q = [q_i \mid i \in [1;n]], q_0, \Sigma = \Sigma_\Sigma \cup \Sigma_\Sigma, \delta, F)$
output : The set $\Sigma_c^n$ as defined in Section 3.2
1 reachable ← arrayInit(m, n);
2 lasts ← arrayInit(n);
3 $\Sigma_c^n \leftarrow \{e\}$;
4 for $i \leftarrow 1$ to $n$ do
5     reachable[i, i] ← 1;
6     lasts[i] ← $q_i$;
7 end
8 foreach $e \in \Sigma_\Sigma$ do
9     $\Sigma_c^n \leftarrow \Sigma_c^n \cup \text{compute}\Sigma_c^n\text{Rec} (\mathcal{A}, c, \text{reachable}, \text{lasts})$;
10 end
```

**Algorithm 1:** Algorithm for computing $\Sigma_c^n$.

Algorithm 1 first initialises $\Sigma_c^n$ to $[e]$. Then, the two arrays reachable and lasts are initialised accordingly, i.e. reachable is filled with 0, with 1 on the diagonal, and lasts[i] is $q_i$. Words are then added to $\Sigma_c^n$ by calling the recursive function compute$\Sigma_c^n$Rec described in Algorithm 2. The array reachable is an array of size $n \times n$, where $n = |Q|$, such that reachable[i, j] is equal to 1 if there is a prefix $w'$ of $w$ such that $q_i$ after $w'$ is $q_j$, and 0 otherwise. The array lasts is an array of size $n$, such that for all $i \in [1;n]$, lasts[i] = $q_i$ after $w$. The function considers recursively all the extensions of $w$, and add them to $\Sigma_c^n$ until the array reachable stabilises, and then returns the computed $\Sigma_c^n$.
Algorithm 2: Function compute$\Sigma_n^\text{Rec}($

The worst-case complexity of Algorithm 1 in terms of assignments is at most $2n + |\Sigma_c|^{n-1}$, where $n = |Q|$. The following algorithms define the primitives of an enforcement mechanism. A state of the enforcement mechanism is represented by a tuple in $V \times V \times \Sigma_1^* \times \Sigma_2^* \times \Sigma_n^* \times \Sigma_n^*$, where $V$ is the set of nodes of the graph $G$ defined in Definition 3.7. The first node is the node reached by the output of the enforcement mechanism (real node). The second node is the strategy node, i.e. the first winning node that can be reached by outputting the first events of the buffer, or the node reached by outputting all the buffer if such a node does not exists. The third member is the buffer composed of the controllable events that have not been output yet. The fourth member is the input, and the fifth is the output.

The first function is enforcerInit (not provided here, due to the lack of space), that returns the initial state of the enforcer, i.e. ($\langle q_0, e \rangle, \langle q_0, e \rangle, e, e, e$).

Function enforcerEventReceived computes the next state of the enforcer after the reception of an event. If the event is controllable, then only the strategy node is updated; if the event is uncontrollable, then it is immediately emitted and the real node is changed accordingly, then the strategy node is computed from this new node. The time complexity of this function is linear in the size of the buffer.

Algorithm 3: Main algorithm to enforce a property

Function enforcerGetStrat returns the strategy to follow. If the strategy node is ahead of the real node, and it is a winning node, then the strategy is to emit the first event of the buffer. Otherwise, the strategy is not to emit. This function has a constant time complexity.

Function enforcerEmit emits the first event of the buffer. The real node is updated accordingly, and the strategy node is unchanged except if the real node caught up with it (i.e. they are equal), in which case the strategy node is updated accordingly. The time complexity of this function is linear in the size of the buffer.
enforcerEventReceived. Then, the enforcer emits a maximal number of events from its buffer with enforcerEmit, i.e. until enforcerGetStrat indicates that is should not emit. Note that emitting events is done by adding the events to the output of the enforcer. The time complexity of this algorithm between two calls to read is linear in the size of the buffer, and thus does not depend on the size of the automaton.

4.2 Implementation
We implemented the algorithms in the C programming language. Our tool takes as input a file describing an automaton, and reads the events from its standard input. It outputs information on the evolution of the state of the enforcement mechanism as well as a summary of the execution when it has ended on its standard output. This approach allows us to adapt easily the tool in order to use it with off-the-shelf applications. The tool first creates the game graph from the automaton, then solves the Büchi game on it. Then, the enforcement mechanism is initialised, and then used to compute the controllable events that can be emitted. When the end of the input is reached, the tool displays first the input of the enforcement mechanism, then its output and the remaining events of its buffer at the end of the the execution. Lastly, it displays a verdict indicating whether the execution ended in an accepting state of the automaton.

Performance Analysis. We provide some execution times of our tool, running on the example given in the paper (φae). We evaluated it on 20 randomly selected inputs of 20 events each. Table 2 shows the inputs and the corresponding mean times taken by the enforcement mechanism to compute its output after each event. The times are given in nanoseconds. The means have been computed over 100 iterations. The inputs are abbreviated: w stands for Write, i for LockOff, n for LockOn, and a for Auth. The results have been obtained using a computer running Ubuntu 16.04 with a 3.40 GHz Intel Core i7 CPU with 16 GB RAM. In Table 2, all the values have the same order of magnitude, showing that the execution time depends little on the input sequence. Thus, the execution time of our enforcement mechanism is quite stable, which makes it reliable.

5 RELATED WORK AND DISCUSSION
Runtime enforcement was pioneered by the work of Schneider with security automata [15], a runtime mechanism for enforcing safety properties. In [15], 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 [11], a more powerful model of enforcement monitors able to insert and suppress events from the execution, thus permitting to enforce non-safety properties. Later, Falcone et al. proposed more general models where the monitors can be synthesised from regular properties [10]. Another recent approach by Dolzehnko et al. [6] introduces Mandatory Result Automata (MRAs). MRAs extend edit-automata by refining the input-output relationship of an enforcement mechanism and thus allowing a more precise description of the enforcement abilities of an enforcement mechanism in concrete application scenarios. All these approaches do not consider uncontrollable events.

Basin et al. [2] introduced uncontrollable events for security automata [15]. The approach in [2] allows to enforce safety properties where some of the events in the specification are uncontrollable. More recently, they proposed a more general approach [1] related to enforcement of security policies with controllable and uncontrollable events. They presented several complexity results and how to synthesise enforcement mechanisms, but they did not provide a tool implementation.

To our knowledge, two runtime enforcement methods using games have been proposed. In [3], Bloem et al. focus on enforcement of safety properties for reactive hardware systems, i.e. systems with boolean signals as inputs and outputs. They propose a method based on a 2-players safety games in order to synthesise a variant of an enforcement monitor called a safety shield and present a tool implementing this approach. This shield ensures correctness (i.e. soundness), and minimum interference according to a notion of distance permitting to measure the deviation between the output and the input of the shield. More recently, Wu et al. propose in [16] to improve the algorithm of [3] in the way that it takes the best recovery strategy among all possible ones, permitting to minimise the deviation, especially in case of burst errors. These two approaches are limited to safety properties and do not support uncontrollable events.

6 CONCLUSION AND FUTURE WORK
This paper revisits the work done in [13, 14] and introduces another way to compute the behaviour of the defined enforcement mechanisms in case of uncontrollable events using a Büchi game. Thus, we define enforcement monitors at two levels of abstraction, one is functional and the second operational. As in [13, 14], we consider that some events are uncontrollable, meaning that they are only observable by the enforcement monitor, that must output them when they are received. We introduce a different way to compute the behaviour of the enforcement mechanism using a Büchi game, that is equivalent to the behaviour of the enforcement mechanism described in [13, 14]. Given a property, we build a graph over which we solve a Büchi game representing the behaviour of the enforcement mechanism. Even though this graph should have an infinite number of vertices, it is possible to reduce it to a finite number, which allows us to store it. The behaviour of the enforcement mechanism only depends on the “current” vertex in the graph. When receiving an event, the enforcement mechanism only updates the current vertex by following some path in the graph, instead of computing again the set of winning configurations. This reduces the time spent in computing the behaviour of the enforcement mechanism, which is one of the main inconveniences when using enforcement mechanisms on running systems. Computing and storing the graph allows us to compute offline the behaviour of the enforcement mechanism, providing better performance at runtime.

We also provide a new way to describe soundness, compliance and optimality with a global view of the system based on inputs and outputs, and we present an implementation showing the effectiveness of the approach.

As a future work, we intend to investigate the runtime enforcement of timed properties [12] using timed games. We consider using the method introduced in this paper to enforce timed properties, as done in [9] without uncontrollable events and with suppression; and in [13] with uncontrollable events and without suppression. The
### Table 2: Table of the mean execution times of our tool for different inputs

<table>
<thead>
<tr>
<th>Input</th>
<th>Times</th>
</tr>
</thead>
<tbody>
<tr>
<td>f n a w w a a a w a a w f n w n n</td>
<td>1-4, 2010. (Lecture Notes in Computer Science), Howard Barringer, Yliès Falcone, Bernd Finkbeiner, Klaus Havelund, Insup Lee, Gordon J. Pace, Grigore Rosu, Oleg Sokolsky, and Nikolai Tillmann (Eds.), Vol. 6418. Springer, 89–105. DOI: <a href="http://dx.doi.org/10.1007/978-3-642-16612-9_9">http://dx.doi.org/10.1007/978-3-642-16612-9_9</a></td>
</tr>
</tbody>
</table>

Graph would be bigger due to the presence of clocks in the automa-
ton performance should be improved. The gain in computation
would be higher, and this would even be more interesting in this set-
ing since it might allow timed properties to be enforced on devices
with little computational power.

### Acknowledgement

The work reported in this article has been done in the context of
the COST Action ARVI IC1402, supported by COST (European Coop-
eration in Science and Technology). It was also partially supported
by French Region Nouvelle Aquitaine, and Bordeaux INP.

### REFERENCES

able Security Policies Revisited. ACM Trans. Inf. Syst. Secur. 16, 1, Article 3
(2013), 26 pages. DOI: [http://dx.doi.org/10.1145/2487222.2487225](http://dx.doi.org/10.1145/2487222.2487225) |

on Runtime Verification (RV 2011) (Lecture Notes in Computer Science), Sarfraz

Shield Synthesis: Runtime Enforcement for Reactive Systems. In Tools and
Algorithms for the Construction and Analysis of Systems - 21st International
Conference, TACAS 2015. Held as Part of the European Joint Conferences on
Proceedings, 533–548. |

Efficient on-the-fly Algorithm for Checking Alternating Timed Simulation. Springer
Berlin Heidelberg, Berlin, Heidelberg, 73–87. DOI: [http://dx.doi.org/10.1007/978-3-642-04368-0_8](http://dx.doi.org/10.1007/978-3-642-04368-0_8) |

for Alternating BÜChi Games. In Proceedings of the Twenty-third Annual ACM-
SIAM Symposium on Discrete Algorithms (SODA ’12), Society for Industrial and
citation.cfm?id=2095116.2095225 |

ment with Mandatory Results Automata. International Journal of Information
Security 14, 1 (Feb. 2015), 47–60. DOI: [http://dx.doi.org/10.1007/s10207-014-0239-8](http://dx.doi.org/10.1007/s10207-014-0239-8) |

cation - First International Conference, RV 2010, St. Julians, Malta, November

---

Conference’17, Matthieu Renard, Antoine Rollet, and Yliès Falcone
A PROOFS OF SECTION 3

In all this section, we will use the notations from Section 3, meaning that \( \varphi \) is a property whose associated automaton is \( A_\varphi = \langle Q, q_0, \Sigma, \rightarrow, \rangle \). In some proofs, we also use notations from Definition 3.10. We also use a functional notation of enforcement functions, i.e. for an enforcement function \( E \) and a word \( \sigma \in \Sigma^* \), we write \( E(\sigma) = \sigma' \) whenever \( (\sigma, \sigma') \in E \).

**Proposition 3.13.** \( E_\varphi \) is an enforcement function as per Definition 3.1.

PROOF. Let us consider \( \sigma \in \Sigma^* \), and \( \sigma' \in \Sigma^* \). If \( \sigma' = \varepsilon \), then \( E_\varphi(\sigma) = E_\varphi(\sigma, \sigma') = E_\varphi(\sigma, \varepsilon) \). Otherwise, let us consider \( (\sigma, \sigma') = store_\varphi(\sigma), a = \sigma'(1) \), and \( (\sigma, \sigma') = store_\varphi(\sigma, a) \). Then, if \( a \in \Sigma_u, \sigma_1 = \sigma, a = \sigma' \), where \( \sigma' \) is defined in Definition 3.10, meaning that \( \sigma_{x_1} \neq \sigma_1 \). If \( a \in \Sigma_c \), then \( \sigma_1 = \sigma, a = \sigma' \), where \( \sigma' \) is defined in Definition 3.10, thus again, \( \sigma_{x_1} \neq \sigma_1 \). In both cases, \( E_\varphi(\sigma) = \sigma_{x_1} \neq \sigma_1 = E_\varphi(\sigma, a) \). Since the order \( \preceq \) is transitive, this means that \( E_\varphi(\sigma) \preceq E_\varphi(\sigma, a) \preceq E_\varphi(\sigma, a, \sigma'(2)) \). Thus \( E_\varphi \) is an enforcement function.

**Lemma A.1.** \( \forall q \in Q, \forall w \in \Sigma^0_n, \langle (q, w, 1) \rangle \in \sigma \implies \langle (q', w', 1) \rangle \in \sigma \).

PROOF. \( W_0 \) is the winning set of the Büchi game for \( P_0 \).

**Lemma A.2.** \( \forall q \in Q, \forall w \in \Sigma^0_n, \langle (q, \sigma, 0) \rangle \in \sigma \implies \langle (q, \sigma) \rangle \).

PROOF. Let us consider \( q \in Q \in \varphi \) and \( \sigma \in \Sigma^0_n \) such that \( \langle (q, \sigma, 0) \rangle \in \sigma \). Then, since \( (q, \sigma, 0) \) is a vertex that belongs to \( P_0 \) that is winning (since it is in \( W_0 \)), this means that there is a winning strategy for \( P_0 \) in the Büchi game. Thus, there is a path in \( G \) that allows us to reach a Büchi state, that is a state in \( F \times \Sigma^\ast_n \). Let us consider \( (q, \sigma) \) such that \( \langle (q, \sigma, 0) \rangle \in \sigma \). Then, if \( \langle (q, \sigma, 0) \rangle \in \sigma \), this means that there is a winning strategy for \( P_0 \) in the Büchi game.

**Proposition 3.14.** \( E_\varphi \) is sound with respect to \( \varphi \in \varphi \) as per Definition 3.2.

PROOF. Let \( P(\varphi) \) be the predicate \( \langle (\sigma, \sigma) = store_\varphi(\sigma) \rangle \implies \langle (\sigma, \sigma) = store_\varphi(\sigma) \rangle \).

**Proposition 3.15.** \( E_\varphi \) is sound with respect to \( \varphi \) in \( \varphi \) as per Definition 3.3.
Thus, following the definition of $\text{G, Reach}(\sigma, a)$ after $\sigma'_a = \text{Reach}(\sigma, a, \sigma)$, $\text{Reach}(\sigma) \notin F$, and $\langle \text{Reach}(\sigma, a) \rangle \text{ after } \sigma'_a, \max_{\langle \sigma' \rangle}(\langle \sigma' \rangle \in \Sigma^*) = \langle \text{Reach}(\sigma), \max_{\langle \sigma' \rangle}(\langle \sigma' \rangle \in \Sigma^*) \rangle$, $\text{Reach}(\sigma) \notin F$. Since $\text{P}(\sigma)$ holds, $\langle \text{Reach}(\sigma, a) \rangle, \sigma'_{\text{Reach}(\sigma, a)} \in \Sigma^*$ and $\text{P}(\sigma)$ holds, this means that $\sigma'_{\text{Reach}(\sigma, a)} = \sigma'_{\text{Reach}(\sigma, a)}$. Since $\text{P}(\sigma)$ holds, this means that $\sigma'_{\text{Reach}(\sigma, a)} = (a, \sigma)_{\in E}$. Thus $\text{P}(\sigma)$ holds.

Case 2: $a \in \Sigma$. Then $\sigma_a' = \sigma'_a$, where $\sigma_a'$ is defined in Definition 3.10, and $\sigma_a' = \sigma'_a = (a, \sigma)_{\in E}$. Therefore, $\sigma_a'_{\text{Reach}(\sigma, a)} = (a, \sigma)_{\in E}$. Since $\sigma_a'$ holds, this means that $\sigma_a'_{\text{Reach}(\sigma, a)} = (a, \sigma)_{\in E}$. Hence, $\text{P}(\sigma)$ holds, this means that $\sigma_a'_{\text{Reach}(\sigma, a)} = (a, \sigma)_{\in E}$. Thus $\text{P}(\sigma)$ holds.

In both cases, $\text{P}(\sigma)$ holds.

By induction on $\sigma$, for all $\sigma \in \Sigma^*$, $(\sigma, \sigma) = \text{store}_E(\sigma) \implies (\sigma, \sigma) = \text{store}_E(\sigma) \implies (\sigma, \sigma) = \text{store}_E(\sigma) \implies (\sigma, \sigma) = \text{store}_E(\sigma) \implies \text{store}_E(\sigma)$.

Moreover, if $\sigma \in \Sigma^*$, $\sigma = \text{store}_E(\sigma)$, and $(\sigma, \sigma) = \text{store}_E(\sigma)$, then $\sigma_t = \text{store}_E(\sigma)$, and $(\sigma, \sigma) = \text{store}_E(\sigma)$, it follows that $\text{P}(\sigma)$ holds. This is true.

Thus $\text{P}(\sigma)$ holds.

PROPOSITION 3.16. $\text{E}_P$ is optimal in $\text{Pre}(\phi)$, as per Definition 3.4.

PROOF. Let $E$ be an enforcement function such that $\text{comp}(E, \Sigma, \Sigma_0)$ holds, and let us consider $\sigma \in \text{Pre}(\phi)$ and $a \in \Sigma$ such that $E(\sigma) = \text{E}_P(\sigma)$ and $|E(\sigma)| > |\text{E}_P(\sigma)|$. Let us also consider $(\sigma, \sigma) = \text{store}_E(\sigma)$. Let us show that there exists $\sigma_u \in \Sigma^*$ such that $E(\sigma, \sigma, \sigma, \sigma) \neq E(\sigma, \sigma, \sigma, \sigma)$.

Case 1: $a \in \Sigma$. Then, since $E$ is compliant, and $E(\sigma) = \text{E}_P(\sigma)$, there exists $\sigma_u \in \Sigma^*$ such that $E(\sigma, a, a, \sigma_u) = E(\sigma, a, a, \sigma_u)$. Moreover, there exists $\sigma_u \in \Sigma^*$ such that $E(\sigma, a, a, \sigma_u) \neq E(\sigma, a, a, \sigma_u)$. Since $E(\sigma)$ is a winning strategy for $(\sigma, \sigma, \sigma, \sigma)$, it follows that $(\sigma, \sigma, \sigma, \sigma)$ is a winning strategy for $(\sigma, \sigma, \sigma, \sigma)$. Following the definition of $G$, this means that either $\sigma_u \neq \sigma_u$, or $\text{Reach}(\sigma, a, a, \sigma_u) \neq \text{Reach}(\sigma, a, a, \sigma_u)$. Since $(\sigma, \sigma, \sigma, \sigma)$ is a winning strategy for $(\sigma, \sigma, \sigma, \sigma)$, it follows that $\sigma_u \neq \sigma_u$, or $\text{Reach}(\sigma, a, a, \sigma_u) \neq \text{Reach}(\sigma, a, a, \sigma_u)$. Since $E(\sigma)$ is a winning strategy for $(\sigma, \sigma, \sigma, \sigma)$, it follows that $\sigma_u \neq \sigma_u$, or $\text{Reach}(\sigma, a, a, \sigma_u) \neq \text{Reach}(\sigma, a, a, \sigma_u)$.

In particular, for all $\sigma \in \Sigma^*$ and $0 < |\phi| < \infty$, $E(\sigma, \sigma, \sigma, \sigma) = E(\sigma, \sigma, \sigma, \sigma)$. This is true.

PROPOSITION 3.15. $\text{E}_P$ is compliant, as per Definition 3.3.

PROOF. For $\sigma \in \Sigma^*$, let $\text{P}(\sigma)$ be the predicate: "$(\sigma, \sigma, \sigma, \sigma)$ is a winning strategy for $(\sigma, \sigma, \sigma, \sigma)$". Let us prove that for all $\sigma \in \Sigma^*$, $\text{P}(\sigma)$ holds.

Induction basis: $\text{store}_E(\sigma) \implies (\sigma, \sigma, \sigma, \sigma) = \text{store}_E(\sigma)$. Let us prove that for all $\sigma \in \Sigma$, $\text{P}(\sigma)$ holds.

Induction step: Let us suppose that for $\sigma \in \Sigma^*$, $\text{P}(\sigma)$ holds. Let us consider $(\sigma, \sigma) = \text{store}_E(\sigma)$, $a \in \Sigma$, and $(\sigma, \sigma) = \text{store}_E(\sigma)$. Let us prove that $\text{P}(\sigma)$ holds.

Case 1: $a \in \Sigma$. Then, $\sigma_a' = \sigma_a.\sigma_a'$, where $\sigma_a'$ is defined in Definition 3.10, and $\sigma_a' = (a, \sigma)_{\in E}$. Therefore, $\sigma_a'_{\text{Reach}(\sigma, a)} = (a, \sigma)_{\in E}$, since $\sigma_a' \in \Sigma^*$. Thus $\text{P}(\sigma)$ holds.
Case 2: \( a \in \Sigma_c \). The proof is the same as in the case where a \( \in \Sigma_u \), by replacing occurrences of “\( \sigma_a, a \)” by “\( \sigma_a \)”, and occurrences of “\( \sigma_a, a \)” by “\( \sigma_a \)”.

Thus, if \( E \) is an enforcement function such that there exists \( \sigma \in \text{Pre}(\varphi) \), and \( a \in \Sigma \) such that \( \text{compliant}(E, \Sigma_u, \Sigma_c, E(\sigma) = \text{E}(\sigma)) \), and \( |E(\sigma,a)| \geq |\text{E}(\sigma,a)| \), then there exists \( \sigma_0 \in \Sigma^*_a \) such that \( E(\sigma,a,\sigma_0) \not\in \varphi \).

This means that \( E_\varphi \) is optimal in \( \text{Pre}(\varphi) \). □

**Proposition 3.18.** 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 \( w \in \Gamma^{E_\varphi} \), we note \( \text{input}(w) = \Pi_1(w(1)) \Pi_1(w(2)) \cdots \Pi_1(w(|w|)) \), the word obtained by concatenating the first members (the inputs) of \( w \). In a similar way, we note \( \text{output}(w) = \Pi_1(w(1)) \Pi_1(w(2)) \cdots \Pi_1(w(|w|)) \), the word obtained by concatenating all the third members (outputs) of \( w \). Since all configurations are not reachable from \( c_0^E \) for \( w \in \Gamma^E \), we note Reach\((w) = c \) whenever \( c^E_0 \rightarrow^E w \rightarrow^E c \), and Reach\((w) = \perp \) if such a \( c \) does not exist. We also define the Rules function as follows:

\[ \text{Rules: } \Sigma^* \rightarrow \Gamma^{E_\varphi} \]

\[ \sigma \mapsto \max_{<}(w \in \Gamma^{E_\varphi} | \text{input}(w) = \sigma \land \text{Reach}(w) \neq \perp) \]

For a word \( \sigma \in \Sigma^*_a \), 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\((\sigma) = \text{output}(\text{Rules}(\sigma)) \). We also note \( e \) the empty word of \( \Sigma^* \), and \( e^E \) the empty word of \( \Gamma^{E_\varphi} \).

For \( \sigma \in \Sigma^*_a \), let \( P(\sigma) \) be the predicate: “\( E_\varphi(\sigma) = \text{output}(\sigma) \land ((\sigma_0, \sigma_c) = \text{store}_\varphi(\sigma) \land \text{Reach}(\text{Rules}(\sigma)) \Rightarrow (q = \text{Reach}(\sigma) \land \sigma_c = \sigma^E_0)) \)”. Let us prove by induction that for all \( \sigma \in \Sigma^*_a \), \( P(\sigma) \) holds.

- **Induction basis:** \( E_\varphi(e) = e = \text{output}(e) \). Moreover, \( \text{store}_\varphi(e) = (e, e) \), and Reach\((E^E) = c^E_0 \). Therefore, as \( c^E_0 = (q_0, e) \), \( P(e) \) holds, because Reach\((e) = q_0 \).

- **Induction step:** Let us suppose now that for some \( \sigma \in \Sigma^*_a \), \( P(\sigma) \) holds. Let us consider \( (\sigma_0, \sigma_c) = \text{store}_\varphi(\sigma) \), \( q = \text{Reach}(\sigma) \), \( a \in \Sigma \), and \( (\sigma, \sigma_q) = \text{store}_\varphi(\sigma,a) \). Let us prove that \( P(\sigma,a) \) holds.

Since \( P(\sigma) \) holds, Reach\((\text{Rules}(\sigma)) = (q, \sigma) \), and \( \sigma_s = \text{output}(\sigma) \). We consider two cases:

**Case 1:** \( a = \perp \). Then, considering \( \sigma'_a = (\sigma,a)^{-1}.\sigma_a = \sigma_s.a.\sigma^c_a. \) Since \( a \in \Sigma_u \), rule pass-uncont can be applied: let us consider \( q' = q \) after \( a \). Then, \( (q, \sigma) \xrightarrow{a/\text{pass-uncont}} (a/q', \sigma) \). Then, if \( \sigma'_a \neq \epsilon \), \( G(q', \sigma) = \emptyset \) or \( G(q', \sigma) = \{e\} \), meaning that no other rule can be applied, and thus \( P(\sigma,a) \) would hold. Otherwise, \( \sigma'_a \neq \epsilon \), and thus \( \sigma'_a \in G(q', \sigma) \), meaning that \( G(q', \sigma) \neq \emptyset \). If \( \sigma'_a \neq \emptyset \), \( \sigma'_a \in G(q, \sigma) \), \( q = \text{reach}(G^E) \), meaning that rule dump\((\sigma) \) can be applied again. Rule dump can actually be applied \( |\sigma'_a| \) times, since for all \( w \in \sigma'_a \), if \( w \neq \sigma'_a \), then \( w^{-1}.\sigma'_a \neq \epsilon \) and \( w^{-1}.\sigma'_a \in G(q' \text{ after } w, w^{-1}.\sigma_c) \). Thus, after rule dump has been applied \( |\sigma'_a| \) times, the configuration reached is \( (q' \text{ after } \sigma'_a, \sigma^{-1}_a.\sigma) \). Moreover, the output produced by all the rules dump is \( \sigma'_a \). Since no rule can be applied after \( |\sigma'_a| \) applications of the rule dump, \( \text{output}(\sigma,a) = \text{output}(\sigma).a.\sigma'_a = \sigma, \) and \( \text{Reach}(\text{Rules}(\sigma,a)) = (q' \text{ after } \sigma'_a, \sigma^{-1}_a.\sigma) = \text{output}(\sigma,a) \). Thus, if \( a = \perp, P(\sigma,a) \) holds.

**Case 2:** \( a = \perp_a \). Then, considering \( \sigma'_a = \sigma^{-1}_a.\sigma, \) \( \sigma_a = \sigma_a.\sigma' \). Since \( a \in \Sigma_u \), it is possible to apply the store-cont rule, and \( (q, \sigma) \) after \( a/\text{store-cont} \). Then as in the case where \( a \in \Sigma_u \), rule dump can be applied \( |\sigma'_a| \) times, meaning that the configuration reached would then be \( (q \text{ after } \sigma_a(1), \sigma_a(2), \ldots (\sigma_a(|\sigma_a|)) ) \). Since \( \sigma_a \neq \emptyset \), \( \text{Reach}(\text{Rules}(\sigma,a)) = (q \text{ after } \sigma_a, \sigma^{-1}_a.\sigma) \). Thus, if \( a = \perp_a \), \( \sigma_a \neq \emptyset \), \( P(\sigma,a) \) holds.

Thus, by induction on \( \sigma \), for all \( \sigma \in \Sigma^*_a \), \( P(\sigma) \) holds. In particular, for all \( \sigma \in \Sigma^*_a, P(\sigma) = \text{output}(\sigma) \). □

**B PROOFS OF SECTION 4**

**B.1 Proofs of termination and complexity**

Algorithm 1 terminates because the array reachable contains only 0 and 1, and in \( \text{compute}_c \), all the subsequent arrays contain more 1 than the previous ones. Since reachable is finite, there exists only a finite number of arrays that can be considered in this way, and thus the array stabilises at some point. Since \( \Sigma_c \) is finite, the algorithm terminates.

Let us now compute the worst-case complexity of Algorithm 1 in terms of assignments. The loop starting in line 4 makes \( n + 1 \) assignments, and the other starting in line 8 makes \( |\Sigma_c| \) assignments, and calls \( |\Sigma_c| \) times function \( \text{compute}_c \). Let us compute the worst-case complexity of function \( \text{compute}_c \). The loop starting in line 5 makes \( n \) assignments, since it is possible to compute \( j \) in constant time (the automaton is deterministic and complete). The assignment in line 4 makes \( n^2 \) assignments, and there is another assignment in line 10. Thus, the loop starting in line 3 makes \( |\Sigma_c| + (n^2 + n^2) \) assignments, which is the complexity of the function. Now, since the first parameter of all the recursive calls is always the same, and the complexity depends only on it, the number of calls made to \( \text{compute}_c \) only depends on the depth of the call stack. The algorithm terminates when reachable stabilises, which must occur in at most \( n - 1 \) calls, since this is the number of 0s present in reachable at the beginning. Thus, the depth of the call stack is bounded by \( n^2 - n \). Thus, the worst-case complexity of Algorithm 1 is at most \( 2n + |\Sigma_c|n^2 - n \). Note that this complexity is computed considering that initialisations have a complexity of 0.

The complexities of the other algorithms are straightforward.