Computational Complexity for State-Feedback Controllers with Partial Observation

Gabriel Kalyon, Tristan Le Gall, Hervé Marchand, Thierry Massart

2009 IEEE International Conference on Control and Automation
Christchurch, New Zealand, December 9-11, 2009

Computational Complexity for State-Feedback Controllers with Partial Observation

Gabriel Kalyon, Tristan Le Gall, Hervé Marchand and Thierry Massart

Abstract— **We study the computational complexity of several decision and optimization control problems arising in partially observed discrete event systems. These problems are related to the state avoidance problem where one must compute a controller which prevents the system from accessing a set of bad states and which is maximal for a defined criterion, based on inclusion of the set of states remaining reachable after the control. We focus our study on memoryless controllers.**

Keywords: Discrete Event Systems, Controller Synthesis, Partial Observation, Computational Complexity.

I. Introduction

Controller synthesis of discrete event systems (DES) has been widely studied these last twenty years [1]. In the particular case of the state avoidance control problem, the controller $\mathcal{C}$ is *valid* for some DES $\mathcal{T}$ and a set of states Bad, if $\mathcal{C}$ prevents $\mathcal{T}$ from reaching any state of Bad. Of course validity is not sufficient to have a valuable solution and *permissiveness* criteria [4], [9] allow to discuss the quality of the solutions and to select the optimal one for the selected criterion. Unfortunately in general, the controller has only a *partial* (or *imperfect*) view of the system, since in practice the observing material of the system to control has a limited precision and some parts of the system can just not be observed. This *partial observation* makes the problem more difficult since in general, as we will see, it is no longer possible to find the optimal controller and the algorithms are hard.

In this paper, we study the synthesis of valid and "best possible" controllers for partially observed discrete event systems. We follow the approach taken by [6], where the partial observation is modeled by a mask, corresponding to a mapping from the state space to an observation space, and we consider state-feedback controllers, whose control is based on the current state of the system [12], rather than on the string of events executed by it (event-feedback controllers). Compared to the event approach, the state-feedback control approach does not receive a lot of attention in the literature; but, in particular cases, it has been seen to require a reduced computational complexity for partially observed and non-deterministic systems [3]. We therefore formalize our state-based approach and study the complexity of various interesting problems in this setting. More precisely, given two controllers $\mathcal{C}_1$ and $\mathcal{C}_2$, we give a definition to say that $\mathcal{C}_1$ is "better" than $\mathcal{C}_2$. The used model and the definition of permissiveness are formalized in section II. In section III, we then define the precise control problems that we study. We motivate and formalize several synthesis or decision questions one may want to solve or answer, such as maximality of a valid controller. We then study, in sections IV and V, the complexity of these problems and show that they are hard or that no polynomial algorithm can solve them unless P = NP (where P stands for deterministic polynomial time and NP stands for nondeterministic polynomial time).

Related works: The *computational complexity of event-feedback controller synthesis* received a lot of attention in the literature. *Under full observation*, it is proven in [2] that the problem of deciding if there exists a controller such that the accepted language of the corresponding controlled system is included in a desired behavior is NP-hard when the system to control is composed of several concurrent systems or when the desired language is the intersection of several languages. *Under partial observation on the actions*, Tsitsiklis proves in [10] that the problem of deciding if there exists a controller such that the behavior of the corresponding controlled system lies between two languages (of actions) cannot be solved in polynomial time (unless P = NP). When both languages are equal, this problem can be solved in polynomial time for the centralized [10] and decentralized [8] cases. Note that we cannot use a transformation from these problems to the problems we are interested in, because the transformation would be exponential.

The *state-feedback controller synthesis* receives only recently more attention. Given a set of allowable states Q, a controller with *full observation*, whose resulting controlled system is the supremal subset of Q, can be computed in polynomial time [11]. In [9], properties of *M-controllability* give a necessary and sufficient condition to synthesize a controller with *partial observation*, whose resulting controlled system achieves exactly a set of allowable states Q. When this behavior cannot be achieved, the authors propose an algorithm to synthesize a controller, whose resulting controlled system is a subset of Q. Both algorithms have a polynomial complexity. Unfortunately, the second one does not always give a maximal solution w.r.t. set inclusion. Then, a natural question is to know if there exists an *efficient* algorithm to synthesize a maximal solution. In [3], the authors generalize the results of [9] using a mask, which is a covering (overlapping sets of indistinguishable states) of

Gabriel Kalyon, Tristan Le Gall and Thierry Massart are with the Université Libre de Bruxelles (U.L.B.), First.Last@ulb.ac.be

Hervé Marchand is with the IRISA/INRIA, Campus de Beaulieu, Rennes, France, First.Last@irisa.fr

G. Kalyon is supported by the Belgian National Science Foundation (FNRS) under a FRIA grant.

This work has been done in the MoVES project (P6/39) which is part of the IAP-Phase VI Interuniversity Attraction Poles Programme funded by the Belgian State, Belgian Science Policy.

the state space instead of a partition, and a non-deterministic system to control. The computational complexity of their algorithm is also polynomial.

II. Framework

We define in this section, the underlying model of discrete-event systems and the notion of permissiveness.

A. Discrete Event Systems

Definition 1 (Discrete Event Systems): A discrete event system (DES) is a tuple $\mathcal{T} = \langle \mathcal{D}_V, \mathcal{D}_0, \Sigma, \delta, \mathcal{D}_m \rangle$ where: (i) $\mathcal{D}_V$ is the set of states, (ii) $\mathcal{D}_0 \subseteq \mathcal{D}_V$ is the set of initial states, (iii) Σ is the set of labels, (iv) $\delta : \mathcal{D}_V \times \Sigma \mapsto 2^{\mathcal{D}_V}$ is the transition relation, and (v) $\mathcal{D}_m \subseteq \mathcal{D}_V$ is the set of marked (accepting) states.

Notations: A *predicate* over the domain $\mathcal{D}_V$ is defined as a subset $P \subseteq \mathcal{D}_V$ (the set of states for which the predicate holds). The complement of a set $H \subseteq \mathcal{D}_V$ is denoted by $\overline{H}$. $\mathbb{B} = \{\mathtt{tt}, \mathtt{ff}\}$ denotes the set of Boolean values. $\delta(\nu, \sigma)!$ denotes that δ is defined on $\langle \nu, \sigma \rangle$. $\mathsf{reach}(\mathcal{T}) \subseteq \mathcal{D}_V$ denotes the set of states that are reachable from the initial states of $\mathcal{T}$ and $\mathsf{reach}(\mathcal{T}, \nu) \subseteq \mathcal{D}_V$ (for any $\nu \in \mathcal{D}_V$) the set of states that are reachable from ν in $\mathcal{T}$.

B. Means of Observation.

We consider systems with partial observation, where there is an uncertainty about the real state the system is. This partial observation is formally defined by a set of observations :

Definition 2 (Set of observations): A set of observations of the state space $\mathcal{D}_V$ is a pair $\langle \mathcal{D}_{Obs}, M \rangle$, where $\mathcal{D}_{Obs}$ is the observation space and the mask $M : \mathcal{D}_V \mapsto \mathcal{D}_{Obs}$ gives for each state $\nu \in \mathcal{D}_V$ the observation $M(\nu)$ the controller has when the system is in this state.

For each observation $obs \in \mathcal{D}_{Obs}$, $M^{-1}(obs)$ gives the set of states ν such that $M(\nu) = obs$. One can notice that the mask M is a partition of the state space; but, the results we prove in this paper hold even when M is a covering [3], [4] of the state space.

C. Means of Control.

Following the Ramadge & Wonham Theory [7], [1], we want adjoin a controller $\mathcal{C}$, which interacts with the system $\mathcal{T}$ in a feedback manner as illustrated in Fig. 1: the controller observes the system and according to his observation delivers the set of events that have to be disabled in order to ensure the desired properties on the system. The control is performed by means of *controllable events*. The alphabet Σ is partitioned into the set of controllable events Σ_c and the set of uncontrollable events Σ_{uc}; only controllable events can be forbidden by the controller. In our case, the controller aims to restrict the system's behavior to ensure a forbidden state invariance property (i.e. to prevent the system from reaching a *bad* state). The controller with partial observation is formally defined as follows:

Definition 3 (Controller): Given a DES $\mathcal{T} = \langle \mathcal{D}_V, \mathcal{D}_0, \Sigma, \delta, \mathcal{D}_m \rangle$, and a set of observations $\langle \mathcal{D}_{Obs}, M \rangle$, a controller for $\mathcal{T}$ is a pair $\mathcal{C} = \langle \mathcal{S}, E \rangle$, where:

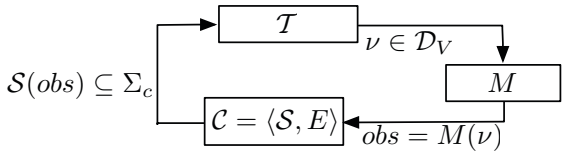

Fig. 1. Control under partial information

- $\mathcal{S} : \mathcal{D}_{Obs} \mapsto 2^{\Sigma_c}$ is a supervisory function which defines, for each observation $obs \in \mathcal{D}_{Obs}$, the set $\mathcal{S}(obs)$ of controllable actions that have to be forbidden when obs is observed by the controller.
- $E \subseteq \mathcal{D}_V$ is a set of states to forbid, which restricts the set of initial states[1].

The controller is memoryless, i.e. the current observation of the system is maintained until the arrival of the next one.

The controlled system resulting from the feedback interaction between the system to control and the controller is given by a DES whose transition relation and set of initial states are restricted :

Definition 4 (Controlled DES): Given a DES $\mathcal{T} = \langle \mathcal{D}_V, \mathcal{D}_0, \Sigma, \delta, \mathcal{D}_m \rangle$, a set of observations $\langle \mathcal{D}_{Obs}, M \rangle$, and a controller $\mathcal{C} = \langle \mathcal{S}, E \rangle$, the system $\mathcal{T}$ controlled by $\mathcal{C}$, is a DES $\mathcal{T}_{/\mathcal{C}} = \langle \mathcal{D}_V, (\mathcal{D}_0)_{/\mathcal{C}}, \Sigma, \delta_{/\mathcal{C}}, \mathcal{D}_m \rangle$, where:

- $(\mathcal{D}_0)_{/\mathcal{C}} = \mathcal{D}_0 \setminus E$
- $\delta_{/\mathcal{C}} : \mathcal{D}_V \times \Sigma \mapsto 2^{\mathcal{D}_V}$ is defined by: $[(\nu' \in \delta(\nu, \sigma)) \wedge (\sigma \notin \mathcal{S}(M(\nu)))] \Rightarrow (\nu' \in \delta_{/\mathcal{C}}(\nu, \sigma))$. An action σ can no longer be fired from a state ν, if σ is forbidden by control in the observation state of ν.

D. Permissiveness

The notion of permissiveness has been introduced to compare the quality of different controllers for a given DES. An obvious definition is :

Definition 5 (Permissiveness): Given a DES $\mathcal{T}$, and a set of observations $\langle \mathcal{D}_{Obs}, M \rangle$, a controller $\mathcal{C}_1$ is more permissive than a controller $\mathcal{C}_2$ iff $\mathsf{reach}(\mathcal{T}_{/\mathcal{C}_2}) \subseteq \mathsf{reach}(\mathcal{T}_{/\mathcal{C}_1})$. When the inclusion is strict, we say that $\mathcal{C}_1$ is strictly more permissive than $\mathcal{C}_2$.

Indeed, in our settings, it seems more coherent to define the permissiveness w.r.t the states that are reachable in the controlled system, rather than w.r.t. the language of the actions that can be fired in the controlled system, since the observations are (masked) states of the system and not actions. However, we will see that in general, no optimal controller exists. Notice also that two controlled systems with the same reachable state space can have different enabled transitions[2].

Usually, when designing the controller, it may be asked that the controlled system is deadlock free or non-blocking :

Definition 6 (Deadlock Free System): Given a DES $\mathcal{T} = \langle \mathcal{D}_V, \mathcal{D}_0, \Sigma, \delta, \mathcal{D}_m \rangle$, a state $\nu \in \mathcal{D}_V$ is deadlock free if $\exists \sigma \in$

[1]We suppose that the controller can restrict the set of initial states of the system in order to prevent it from starting its execution in a bad state.

[2]We could have used an extended definition of permissiveness where if two controlled systems have equal reachable state space, inclusion of the transitions that can be fired from reachable states is also taken into account

$\Sigma : \delta(\nu, \sigma)!$. Moreover, the system $\mathcal{T}$ is deadlock free if all the reachable states of $\mathcal{T}$ are deadlock free.

Definition 7 (Non-blocking System): Given a DES $\mathcal{T} = \langle \mathcal{D}_V, \mathcal{D}_0, \Sigma, \delta, \mathcal{D}_m \rangle$, a state $\nu \in \mathcal{D}_V$ is non-blocking if $\mathsf{reach}(\mathcal{T}, \nu) \cap \mathcal{D}_m \neq \varnothing$. Moreover, the system $\mathcal{T}$ is non-blocking if all the reachable states of $\mathcal{T}$ are non-blocking.

III. Definition of the Problems

We start from the State Avoidance Control Problem ($SACP$), where given a set Bad of forbidden states and a system $\mathcal{T}$ to control, the problem consists in synthesizing a controller $\mathcal{C}$, which prevents the controlled system $\mathcal{T}_{/\mathcal{C}}$ from reaching Bad. In [11], the author proves that if $\mathcal{T}$ is fully observed, there is a most permissive controller solving SACP. This uniqueness result however does not hold when the controller only has a partial observation of the system [4].

In this framework, our goal is thus to find a *maximal* solution, i.e. a solution such that no other solution is strictly more permissive. This problem is called Maximal State Avoidance Control Problem (M_{SACP}) and is formally defined by:

Problem 1 (M_{SACP}): For a DES $\mathcal{T}$, a set of observations $\langle \mathcal{D}_{Obs}, M \rangle$ and a predicate Bad, which gives a set of forbidden states, the maximal state avoidance control problem consists in computing a controller $\mathcal{C} = \langle \mathcal{S}, E \rangle$ such that (*safety*) $\mathsf{reach}(\mathcal{T}_{/\mathcal{C}}) \cap Bad = \varnothing$ and (*maximality*) no controller $\mathcal{C}' = \langle \mathcal{S}', E' \rangle$, satisfying this condition, is strictly more permissive than $\mathcal{C}$.

In the following, we say that a controller $\mathcal{C}$ is *valid* if it satisfies the property $\mathsf{reach}(\mathcal{T}_{/\mathcal{C}}) \cap Bad = \varnothing$.

In section IV, we show that this problem is *difficult* to solve when system $\mathcal{T}$ is finite, and is even *undecidable* [4] when system $\mathcal{T}$ is infinite. Therefore, we may wonder whether a given controller $\mathcal{C}$ (obtained for example by an approximation algorithm) defines a *good solution*.

Several criteria may define what a good solution is:

1) no another valid controller $\mathcal{C}'$ exists such that, for the system $\mathcal{T}$, $\mathcal{C}'$ is strictly more permissive than $\mathcal{C}$
2) in the controlled system $\mathcal{T}_{/\mathcal{C}}$, a given set of states *Min* is reachable ($\varnothing \neq \mathit{Min} \subseteq \mathcal{D}_V$)

We may wonder, in each case, how difficult it is to determine if $\mathcal{C}$ satisfies one of those criteria. The problem related to the first criterion is named Maximal State Avoidance Control Decision Problem ($M_{SAC}D_P$) and is defined by:

Problem 2 ($M_{SAC}D_P$): For a DES $\mathcal{T}$, a set of observations $\langle \mathcal{D}_{Obs}, M \rangle$, a predicate Bad, which gives a set of forbidden states, and a valid controller $\mathcal{C} = \langle \mathcal{S}, E \rangle$, the maximal state avoidance control decision problem consists in deciding if $\mathcal{C}$ is maximal, i.e. if there exists no valid controller $\mathcal{C}'$ such that $\mathcal{C}'$ is strictly more permissive than $\mathcal{C}$.

The problem related to the second criterion is named Interval State Avoidance Control Problem (I_{SACP}) and is defined by:

Problem 3 (I_{SACP}): For a DES $\mathcal{T}$, a set of observations $\langle \mathcal{D}_{Obs}, M \rangle$ and non-empty predicates *Min* and *Max*, which give the minimum and the maximum set of allowable states, the interval state avoidance control problem consists in deciding if there exists a controller $\mathcal{C} = \langle \mathcal{S}, E \rangle$ such that $\mathit{Min} \subseteq \mathsf{reach}(\mathcal{T}_{/\mathcal{C}}) \subseteq \mathit{Max}$.

Min can be seen as the minimum admissible behavior and *Max* as the maximum admissible behavior (the controller must prevent from reaching $\overline{\mathit{Max}}$).

In section V, we prove that these problems are also *difficult* to solve. An alternative is then to measure the quality of the controller with a criterion which seems to be weaker than the permissiveness: the number of states which remains reachable after control. Of course this criterion gives limited information since two solutions with the same number of reachable states may be completely different, but one can hope to solve *efficiently* the state avoidance control problem with this simpler criterion of maximality. Unfortunately, this problem is also *difficult* to solve, because we prove in section V that the following problem is NP-complete:

Problem 4 (MC_{SACP}): For a DES $\mathcal{T}$, a set of observations $\langle \mathcal{D}_{Obs}, M \rangle$, and a predicate Bad, which gives a set of forbidden states, the maximal cardinality state avoidance control problem consists in deciding if there exists a valid controller $\mathcal{C} = \langle \mathcal{S}, E \rangle$ such that $|\mathsf{reach}(\mathcal{T}_{/\mathcal{C}})| \geq N$ (where $N \in \mathbb{N}^+$).

In the sequel, we also consider, for all problems defined above, the computational complexity for the cases where the controlled system must be non-blocking and deadlock free.

IV. Complexity of Optimization Problems

In this section, we present complexity results for the Maximal State Avoidance Control Problem, defined in section III, and the deadlock free and non-blocking versions of this problem.

Proposition 1: M_{SACP} is NP-hard.

A reduction of 3SAT into our problem will be used to prove the proposition. Let us first illustrate the principle of the reduction.

Example 1: Let ϕ be a boolean formula in Conjunctive Normal Form (CNF) defined by: $\phi = (p_0 \vee \neg p_1 \vee p_2) \wedge (p_0 \vee \neg p_1 \vee \neg p_1)$.

We would like to construct from ϕ an instance of M_{SACP}, and in particular a DES $\mathcal{T}_\phi = \langle \mathcal{D}_V, \mathcal{D}_0, \Sigma, \delta, \mathcal{D}_m \rangle$, in such a way that a particular state (named $true$) of $\mathcal{T}_\phi$ will be reachable in the controlled system iff ϕ is satisfiable. In our example, ϕ is composed of 2 clauses and 3 variables. The construction is the following:

- we create for each variable p_i ($\forall i \in [0, 2]$) the states[3] $p_i^0, p_i^1, \overline{p_i^1}, p_i^2, \overline{p_i^2}, st_i, st_i'$, for each clause c_i ($\forall i \in [1, 2]$) the states $\ell_{i,1}, \ell_{i,2}, \ell_{i,3}$ (i.e. one state for each literal of the clause) and 4 additional states $st, st', bad, true$ (see Fig. 2).
- the observation space $\mathcal{D}_{Obs} = \{op_0, op_1, op_2, ost\}$. Thus, there is an observation state op_i for each variable p_i of ϕ.

[3]A simpler construction can be defined without the states st_i, st_i', but $\mathcal{T}_\phi$ is then non-deterministic. Thus, these states allow to make the system to control deterministic.

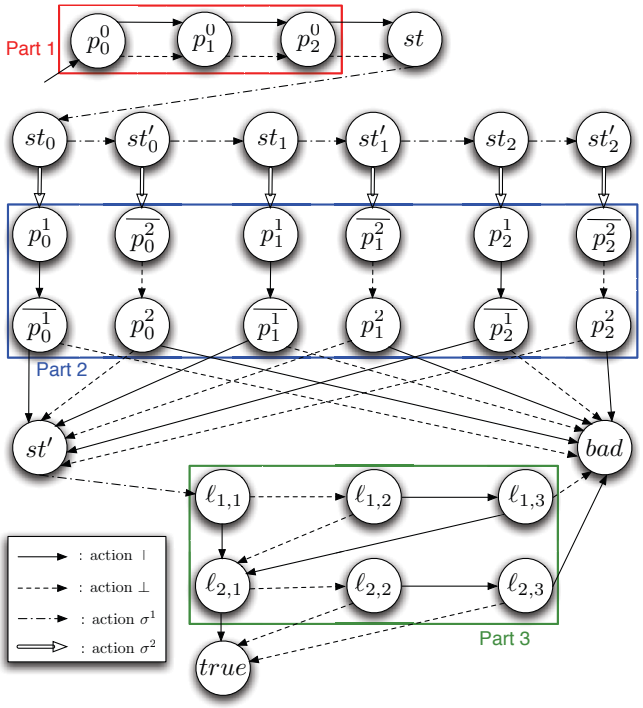

Fig. 2. Construction of $\mathcal{T}_\phi$.

- the states bad, $true$, st, st', st_i, st'_i ($\forall i \in [0,2]$) are indistinguishable (i.e. $M^{-1}(ost) = \{st, st', st_0, st'_0, st_1, st'_1, st_2, st'_2, bad, true\}$) and for each other state, the observation state of its related proposition is observed (for example: $M^{-1}(op_0) = \{p_0^0, p_0^1, \overline{p_0^1}, p_0^2, \overline{p_0^2}, \ell_{1,1}, \ell_{2,1}\}$).
- there are 4 controllable actions $\top$, $\bot$, σ^1, σ^2 (see Fig. 2).

The construction is mainly composed of 3 parts (see Fig. 2):

- with the part 1, a maximal valid controller must allow at least one action (among $\top$ and $\bot$) in op_i ($\forall i \in [0,2]$). Indeed, if not, the controller which forbids no action in op_i ($\forall i \in [0,2]$) and forbids only σ^2 in ost, would be more permissive.
- with the part 2, a maximal valid controller, which allows σ^1 and σ^2 in ost, must forbid at least one action (among $\top$ and $\bot$) in op_i ($\forall i \in [0,2]$). Indeed, if for example $\{\top, \bot\}$ is allowed in op_0, then bad will be reachable from p_0^1 and $\overline{p_0^2}$ (through $\overline{p_0^1}$ and p_0^2) in the controlled system.
- Thus, a maximal valid controller $\mathcal{C} = \langle \mathcal{S}, E \rangle$, which enables σ^1 and σ^2 in ost, must allow exactly one action (among $\top$ and $\bot$) in op_i ($\forall i \in [0,2]$). Then, we can create an one-to-one mapping between the choices of the action to forbid among $\top$ and $\bot$ in these states (the function $\mathcal{S}$) and the valuations $val : \{p_0, p_1, p_2\} \mapsto \mathbb{B}$ (which assign a value to the variables of ϕ). We define this relation as follows: ($\forall i \in [0,2] : \mathcal{S}(op_i) = \{\bot\}$ iff $val(p_i) = \mathsf{tt}$). It means that $\top$ is allowed in op_i iff the value of p_i is tt. So, the part 3 is constructed in such a way that from the state $\ell_{1,1}$, if $\mathcal{S}$ corresponds to a valuation $val \models \phi$ (resp. $val \not\models \phi$), then $true$ is reachable (resp. bad is reachable) in the controlled system. Indeed, if the literal $\ell_{i,j}$ of a clause c_i is valuated to true, then from the state $\ell_{i,j}$ we can reach $\ell_{i+1,j}$ (or $true$ if c_i is the last clause) and if $\ell_{i,j}$ is valuated to false, then from this state we can reach $\ell_{i,j+1}$ (or bad if $\ell_{i,j}$ is the last literal of the clause). For example:
  - if val is such that $val(p_0) = val(p_1) = \mathsf{ff}$ and $val(p_2) = \mathsf{tt}$, then we traverse the states $\ell_{1,1}$, $\ell_{1,2}$, $\ell_{2,1}$, $\ell_{2,2}$ and $true$.
  - if val is such that $val(p_0) = \mathsf{ff}$ and $val(p_1) = val(p_2) = \mathsf{tt}$, then we traverse the states $\ell_{1,1}$, $\ell_{1,2}$, $\ell_{1,3}$, $\ell_{2,1}$, $\ell_{2,2}$, $\ell_{2,3}$ and bad.

  Note that, since bad cannot be reached in M_{SACP}, if the formula is unsatisfiable, Part 3 (hence $true$) will not be reachable in the computed solution.

Proof: **Polynomial transformation from 3SAT to M_{SACP}.** We consider a CNF formula ϕ over a set of variables $\mathcal{P} = \{p_0, \ldots, p_k\}$: $\phi = \bigwedge_{m=1}^{n_c} c_m$, where $n_c > 0$ and the clauses $c_m = \bigvee_{j=1}^{3} \ell_{m,j}$. Each $\ell_{m,j}$ is a variable in $\mathcal{P}$ (positive literal) or the negation of a variable in $\mathcal{P}$ (negative literal). We denote by Cl the set of clauses of ϕ.

An instance of M_{SACP} is built from 3SAT as follows. First, we define the state space $\mathcal{D}_V$, the observation space $\mathcal{D}_{Obs}$ and the set of forbidden states Bad:

1) The domain $\mathcal{D}_V = \{bad, true, st, st'\} \cup \{st_i, st'_i | \forall i \in [0,k]\} \cup \{p_i^0, p_i^1, p_i^2, \overline{p_i^1}, \overline{p_i^2} | \forall p_i \in \mathcal{P}\} \cup \{\ell_{m,1}, \ell_{m,2}, \ell_{m,3} | \forall c_m \in \mathsf{Cl}\}$
2) $\mathcal{D}_{Obs} = \{op_i | \forall p_i \in \mathcal{P}\} \cup \{ost\}$
3) $Bad = \{bad\}$

In the sequel, we denote $\mathcal{O}_\mathcal{P} = \{op_i | \forall i \in [0,k]\}$, the set of observation states, ost excluded.

The states bad, $true$, st, st', st_i, st'_i ($\forall i \in [0,k]$) are indistinguishable and for each other state, the observation state of its related proposition is observed. Formally:

1) $\forall op_i \in \mathcal{O}_\mathcal{P}, M^{-1}(op_i) = \{p_i^0, p_i^1, p_i^2, \overline{p_i^1}, \overline{p_i^2}\} \cup \{\ell_{m,j} | m \in [1,n_c] \wedge j \in [1,3] \wedge ((\ell_{m,j} = p_i) \vee (\ell_{m,j} = \neg p_i))\}$
2) $M^{-1}(ost) = \{st, st', bad, true\} \cup \{st_i, st'_i | \forall i \in [0,k]\}$

Finally, we define the system $\mathcal{T}_\phi = \langle \mathcal{D}_V, \mathcal{D}_0, \Sigma, \delta, \mathcal{D}_m \rangle$ to control. The construction of $\mathcal{T}_\phi$ is such that $true$ will be reachable in the controlled system obtained by the resolution of M_{SACP} iff ϕ is satisfiable. Formally, $\mathcal{T}_\phi$ is defined by:

1) the set $\mathcal{D}_V$ defined above.
2) the set $\mathcal{D}_0 = \{p_0^0\}$.
3) the set of events $\Sigma = \Sigma_c \uplus \Sigma_{uc}$ with $\Sigma_c = \{\top, \bot, \sigma^1, \sigma^2\}$ and $\Sigma_{uc} = \varnothing$. Intuitively, a transition $\delta(x, \top)$ (resp. $\delta(x, \bot)$) represents a valuation $x = \mathsf{tt}$ (resp. $x = \mathsf{ff}$).
4) the transition relation δ defined as follows:
   a) $\forall i \in [0, k-1] : \delta(p_i^0, \top) = \delta(p_i^0, \bot) = \{p_{i+1}^0\}$. Moreover, $\delta(p_k^0, \top) = \delta(p_k^0, \bot) = \{st\}$ (Part 1 of Fig. 2).
   b) $\delta(st, \sigma^1) = \{st_0\}$ and $\forall i \in [0,k] : \delta(st_i, \sigma^1) = \{st'_i\}$ and $\delta(st_i, \sigma^2) = \{p_i^1\}$. Moreover, $\forall i \in [0, k-1]$:

$\delta(st'_i, \sigma^1) = \{st_{i+1}\}$ and $\delta(st'_i, \sigma^2) = \{\overline{p_i^2}\}$. And $\delta(st'_k, \sigma^2) = \{\overline{p_k^2}\}$.

c) $\forall i \in [0,k] : \delta(p_i^1, \top) = \{\overline{p_i^1}\}$, $\delta(\overline{p_i^1}, \bot) = \{bad\}$, $\delta(\overline{p_i^1}, \top) = \{st'\}$, $\delta(\overline{p_i^2}, \bot) = \{p_i^2\}$, $\delta(p_i^2, \top) = \{bad\}$ and $\delta(p_i^2, \bot) = \{st'\}$ (Part 2 of Fig. 2).

d) $\delta(st', \sigma^1) = \{\ell_{1,1}\}$.

e) for the states of the clause c_m ($\forall m \in [1, n_c - 1]$), we define the following transitions:

i) if $\ell_{m,j}$ (for $j = 1, 2$) is a positive literal, $\delta(\ell_{m,j}, \bot) = \{\ell_{m,j+1}\}$ and $\delta(\ell_{m,j}, \top) = \{\ell_{m+1,1}\}$. Otherwise, $\delta(\ell_{m,j}, \top) = \{\ell_{m,j+1}\}$ and $\delta(\ell_{m,j}, \bot) = \{\ell_{m+1,1}\}$.

ii) if $\ell_{m,3}$ is a positive literal, $\delta(\ell_{m,3}, \bot) = \{bad\}$ and $\delta(\ell_{m,3}, \top) = \{\ell_{m+1,1}\}$. Otherwise, $\delta(\ell_{m,3}, \top) = \{bad\}$ and $\delta(\ell_{m,3}, \bot) = \{\ell_{m+1,1}\}$.

f) for the states of the clause c_{n_c}, we define the following transitions:

i) if $\ell_{n_c,j}$ (for $j = 1, 2$) is a positive literal, $\delta(\ell_{n_c,j}, \bot) = \{\ell_{n_c,j+1}\}$ and $\delta(\ell_{n_c,j}, \top) = \{true\}$. Otherwise, $\delta(\ell_{n_c,j}, \top) = \{\ell_{n_c,j+1}\}$ and $\delta(\ell_{n_c,j}, \bot) = \{true\}$.

ii) if $\ell_{n_c,3}$ is a positive literal, $\delta(\ell_{n_c,3}, \bot) = \{bad\}$ and $\delta(\ell_{n_c,3}, \top) = \{true\}$. Otherwise, $\delta(\ell_{n_c,3}, \top) = \{bad\}$ and $\delta(\ell_{n_c,3}, \bot) = \{true\}$.

5) the set $\mathcal{D}_m = \mathcal{D}_V$ (in fact, $\mathcal{D}_m$ can have any value)

The algorithm to decide 3SAT is the following. From the formula ϕ, we build an instance of M_{SACP} as described above. We get a controller $\mathcal{C} = \langle \mathcal{S}, E \rangle$ from an algorithm solving M_{SACP} and we decide that ϕ is satisfiable iff $true \in \mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}})$. If we prove this equivalence, then M_{SACP} is NP-hard, since 3SAT is NP-complete.

Proof of the equivalence: ϕ is satisfiable iff $true \in \mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}})$, where $\mathcal{C}$ is a maximal valid controller.

We first prove that a maximal valid controller $\mathcal{C} = \langle \mathcal{S}, E \rangle$ is such that $\{p_0^0\} \notin E$.

Lemma 1: The controllers $\mathcal{C}_1 = \langle \mathcal{S}_1, E_1 \rangle$, with $\{p_0^0\} \in E_1$, are not maximal.

Proof: $\mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}_1}) = \varnothing$, because the set of initial states in the controlled system is empty, i.e. $(\mathcal{D}_0)_{/\mathcal{C}_1} = \varnothing$. The controller, which forbids only σ^2 in ost is valid and more permissive than $\mathcal{C}_1$. ■

In what follows, we will use the notation IS to denote a subset of $\mathcal{D}_V$ which does not include $\{p_0^0\}$.

Then, we prove that a maximal valid controller must allow at least one action (among $\top$ and $\bot$) in each observation state of $\mathcal{O}_\mathcal{P}$.

Lemma 2: If $\mathcal{C} = \langle \mathcal{S}, \mathsf{IS} \rangle$ is a maximal valid controller, then $\forall op_i \in \mathcal{O}_\mathcal{P} : \mathcal{S}(op_i) \neq \{\top, \bot\}$.

Proof: Suppose there exists $op_i \in \mathcal{O}_\mathcal{P}$ such that $\mathcal{S}(op_i) = \{\top, \bot\}$. Then, $\mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}}) \subset \{p_0^0, p_1^0, \ldots, p_k^0, st\}$. The controller, which forbids only σ^2 in ost is valid and more permissive than $\mathcal{C}$. But, it is a contradiction with the fact that $\mathcal{C}$ is maximal. ■

This property implies that st is reachable in the system controlled by a maximal valid controller.

Now, we prove that a maximal valid controller must forbid at least one action (among $\top$ and $\bot$) in each observation state of $\mathcal{O}_\mathcal{P}$ (if σ^1 and σ^2 are allowed in ost).

Lemma 3: If $\mathcal{C} = \langle \mathcal{S}, \mathsf{IS} \rangle$ is a maximal valid controller and if $\sigma^1, \sigma^2 \notin \mathcal{S}(ost)$, then $\forall op_i \in \mathcal{O}_\mathcal{P} : \mathcal{S}(op_i) \neq \varnothing$.

Proof: Suppose that $op_j \in \mathcal{O}_\mathcal{P}$ is such that $\mathcal{S}(op_j) = \varnothing$. The set $\{p_i^1, \overline{p_i^2} | \forall i \in [0,k]\}$ is reachable in $(\mathcal{T}_\phi)_{/\mathcal{C}}$, because $\sigma^1, \sigma^2 \notin \mathcal{S}(ost)$ and by Lemma 2. In particular, p_j^1 and $\overline{p_j^2}$ are reachable. Since, no action is forbidden in these states, the state bad is reachable from these states (through $\overline{p_j^1}$ and p_j^2). But, it is a contradiction with the fact that $\mathcal{C}$ is valid. ■

For the controllers which forbid exactly one action (among $\top$ and $\bot$) in the states of $\mathcal{O}_\mathcal{P}$, we have an one-to-one mapping between the choices of the action to forbid among $\top$ and $\bot$ in each observation state of $\mathcal{O}_\mathcal{P}$ and the valuations $val : \mathcal{P} \mapsto \mathbb{B}$ (which assign a value to each variable of $\mathcal{P}$). We define this mapping as follows: $\forall i \in [0,k] : (\mathcal{S}(op_i) = \{\bot\}$ iff $val(p_i) = \mathtt{tt})$. It means that $\top$ is allowed in op_i iff the value of p_i is $\mathtt{tt}$.

Lemma 4: Let $\mathcal{C} = \langle \mathcal{S}, \mathsf{IS} \rangle$ be a maximal valid controller. If ϕ is not satisfiable, then $\sigma^1 \notin \mathcal{S}(ost)$ and $\sigma^2 \in \mathcal{S}(ost)$. Hence, $true \notin \mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}})$.

Proof: Suppose that $\sigma^1 \in \mathcal{S}(ost)$, then $\mathcal{C}$ is not maximal, because the controller, which forbids only σ^2 in ost, is more permissive than $\mathcal{C}$.

Now, suppose that $\sigma^2 \notin \mathcal{S}(ost)$. Then, by Lemma 2 and 3, a maximal valid controller must forbid exactly one action among $\top$ and $\bot$ in the states of $\mathcal{O}_\mathcal{P}$ and $\ell_{1,1} \in \mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}})$. Let $val : \mathcal{P} \mapsto \mathbb{B}$ be a valuation. Since, ϕ is not satisfiable, there exists at least one clause $c \in \mathsf{Cl}$ such that $val \not\models c$. Let c_j be this first clause (then $c_1, \ldots, c_{j-1}$ are satisfied by val). Then for all $1 \leq m < j$, c_m is satisfied and by the construction of $\mathcal{T}_\phi$, there exists a path between $\ell_{m,1}$ and $\ell_{m+1,1}$ in the controlled system. But, since $val \not\models c_j$, the state bad is reachable from $\ell_{j,1}$; it is a contradiction. ■

Lemma 5: Let $\mathcal{C} = \langle \mathcal{S}, \mathsf{IS} \rangle$ be a maximal valid controller. If ϕ is satisfiable, then $true \in \mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}})$.

Proof: Let $\mathcal{C}_1 = \langle \mathcal{S}_1, \mathsf{IS} \rangle$ be a controller such that $\sigma^1, \sigma^2 \notin \mathcal{S}_1(ost)$ and the choice of the action to forbid among $\top$ and $\bot$ in the states of $\mathcal{O}_\mathcal{P}$ corresponds to a valuation $val' : \mathcal{P} \mapsto \mathbb{B}$ satisfying ϕ. Such a valuation exists, since ϕ is satisfiable. Now, we prove that $true \in \mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}_1})$. The state $\ell_{1,1}$ is reachable, because $\sigma^1, \sigma^2 \notin \mathcal{S}_1(ost)$. Similarly as above, since each c_m ($1 \leq m < n_c$) is satisfied by val', there exists a path between $\ell_{m,1}$ and $\ell_{m+1,1}$, and bad is not reachable from $\ell_{m,1}$. Moreover, since $val' \models c_{n_c}$, there is a path between $\ell_{n_c,1}$ and $true$, and bad is not reachable from $\ell_{n_c,1}$.

Clearly, $\mathcal{C}_1$ is more permissive than any valid controller $\mathcal{C}_2 = \langle \mathcal{S}_2, \mathsf{IS} \rangle$ with $\sigma^1 \in \mathcal{S}_2(ost)$ or $\sigma^2 \in \mathcal{S}_2(ost)$. Thus, for ϕ satisfiable, a maximal valid controller $\mathcal{C}_3 = \langle \mathcal{S}_3, \mathsf{IS} \rangle$ is such that $\sigma^1, \sigma^2 \notin \mathcal{S}_3(ost)$, and, by Lemma 2 and 3, must forbid exactly one action among $\top$ and $\bot$ in the states of $\mathcal{O}_\mathcal{P}$

By the proof of Lemma 4, the valid controllers $\mathcal{C}_4 = \langle \mathcal{S}_4, \mathsf{IS} \rangle$, whose function $\mathcal{S}_4$ is constructed from a valuation

not satisfying ϕ, are such that $\sigma^1 \in \mathcal{S}_4(ost)$ or $\sigma^2 \in \mathcal{S}_4(ost)$. Indeed, if not, bad would be reachable. In consequence, these controllers cannot be maximal.

Thus, for ϕ satisfiable, the maximal valid controllers $\mathcal{C}_5 = \langle \mathcal{S}_5, \mathsf{IS} \rangle$ are such that $\sigma^1, \sigma^2 \notin \mathcal{S}_5(ost)$ and the choice of the action to forbid among $\top$ and $\bot$ in each state of $\mathcal{O}_\mathcal{P}$ corresponds to a valuation satisfying ϕ. As shown above, $true$ is reachable with these controllers. ■

In conclusion, by Lemma 4 and 5, if $\mathcal{C}$ is a maximal valid controller, then ϕ is satisfiable iff $true \in \mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}})$. ■

One can note that the system $\mathcal{T}_\phi$ is deterministic. Thus, Proposition 1 holds for deterministic systems to control. Moreover, the propositions we prove in the sequel will also hold for deterministic systems.

Now, we can easily obtain the same result for the Deadlock Free Maximal State Avoidance Control Problem (DFM_{SACP}) (i.e. solving M_{SACP} so that the resulting controlled system $\mathcal{T}_{/\mathcal{C}}$ is deadlock free). This problem is also *difficult* to solve.

Proposition 2: DFM_{SACP} is NP-hard.

Proof: The proof consists in a reduction from M_{SACP} to DFM_{SACP}. From $\mathcal{T} = \langle \mathcal{D}_V, \mathcal{D}_0, \Sigma, \delta, \mathcal{D}_m \rangle$, we build the system to control $\mathcal{T}_n = \langle \mathcal{D}_V, \mathcal{D}_0, \Sigma_n, \delta_n, \mathcal{D}_m \rangle$ for the instance of DFM_{SACP}, where:

- $\Sigma_n = \Sigma \cup \{\sigma_n\}$. The new action σ_n is uncontrollable.
- $\forall \nu \in \mathcal{D}_V, \forall \sigma \in \Sigma : \delta_n(\nu, \sigma) = \delta(\nu, \sigma)$. Moreover, $\forall \nu \in \mathcal{D}_V : \delta(\nu, \sigma_n) = \{\nu\}$. Thus, σ_n can be fired from any state $\nu \in \mathcal{D}_V$ and loops on ν.

$\langle \mathcal{D}_{Obs}, M \rangle$ and Bad do not change for the instance of DFM_{SACP}.

Now, we prove the correctness of the polynomial transformation. For that, we show that a controller $\mathcal{C}$ is a solution of M_{SACP} iff it is a solution of DFM_{SACP}. This equivalence holds, because $\mathcal{T}_n$ contains only deadlock free states. ■

The Non-blocking Maximal State Avoidance Control Problem (NbM_{SACP}) (i.e. solving M_{SACP} so that the resulting controlled system $\mathcal{T}_{/\mathcal{C}}$ is non-blocking) is also *difficult* to solve.

Proposition 3: NbM_{SACP} is NP-hard.

Proof: The proof consists in a reduction from M_{SACP} to NbM_{SACP}. From $\mathcal{T} = \langle \mathcal{D}_V, \mathcal{D}_0, \Sigma, \delta, \mathcal{D}_m \rangle$, we build the system to control $\mathcal{T}' = \langle \mathcal{D}_V, \mathcal{D}_0, \Sigma, \delta, \mathcal{D'}_m \rangle$ for the instance of NbM_{SACP}, where $\mathcal{D'}_m = \mathcal{D}_V$. $\langle \mathcal{D}_{Obs}, M \rangle$ and Bad do not change for the instance of NbM_{SACP}.

Now, we prove the correctness of the polynomial transformation. For that, we show that a controller $\mathcal{C}$ is a solution of M_{SACP} iff it is a solution of NbM_{SACP}. This equivalence holds, because $\forall \nu \in \mathcal{D}_V : \nu \in \mathcal{D'}_m$, and thus $\mathcal{T}'$ contains only non-blocking states. ■

V. Complexity of Decision Problems

We demonstrated that M_{SACP} is NP-hard. However, it is quite easy to find a "good" valid controller [3], [4], [9], but without the certainty that it is a maximal one. In Section III, we gave some quality criteria and defined the problems related to those criteria. We now give complexity results for those decision problems.

A. Maximal State Avoidance Control Decision Problem

Proposition 4: $M_{SAC}D_P$ is coNP-complete.

Proof: We prove that the complementary problem of $M_{SAC}D_P$ (named $\overline{M_{SAC}D_P}$), which consists in deciding if there exists a valid controller $\mathcal{C}'$ strictly more permissive than $\mathcal{C}$, is NP-complete.

First, we prove that $\overline{M_{SAC}D_P} \in$ NP. Given $\mathcal{T}$, $\langle \mathcal{D}_{Obs}, M \rangle$, Bad and $\mathcal{C}$, we select a controller $\mathcal{C}' = \langle \mathcal{S}', E' \rangle$, and test that $\mathcal{C}'$ is valid and strictly more permissive than $\mathcal{C}$. These properties can be verified in polynomial time. If $\mathcal{C}'$ satisfies these properties, then it is a solution to $\overline{M_{SAC}D_P}$. Therefore, $\overline{M_{SAC}D_P} \in$ NP.

The second part of the proof consists in a reduction from 3SAT to $\overline{M_{SAC}D_P}$. An instance of $\overline{M_{SAC}D_P}$ is built from 3SAT as follows. The system to control $\mathcal{T}_\phi$, the set of observations $\langle \mathcal{D}_{Obs}, M \rangle$ and the set Bad are built as in the proof of Proposition 1. The controller $\mathcal{C} = \langle \mathcal{S}, \varnothing \rangle$ is built as follows for the supervisory function $\mathcal{S}$:

$$S(obs) = \begin{cases} \varnothing & \text{if } obs \in \mathcal{O}_\mathcal{P} \\ \{\sigma^2\} & \text{if } obs = ost \end{cases}$$

Now, we prove the correctness of the polynomial transformation. For that, we show that ϕ is satisfiable iff there exists a valid controller $\mathcal{C}'$ strictly more permissive than $\mathcal{C}$. This equivalence is proven as follows:

- If ϕ is not satisfiable, then there exists no valid controller $\mathcal{C}'$ strictly more permissive than $\mathcal{C}$. Indeed, by Lemma 4, if ϕ is not satisfiable, then a maximal valid controller allows σ^1 in ost and forbids σ^2 in ost. In consequence, $\mathcal{C}$ is a maximal valid controller.
- If ϕ is satisfiable, then there exists a valid controller $\mathcal{C}'$ strictly more permissive than $\mathcal{C}$. Indeed, the controller $\mathcal{C}_1$ defined in the proof of Lemma 5 is valid and strictly more permissive than $\mathcal{C}$. ■

The deadlock free ($DFM_{SAC}D_P$) and non-blocking ($NbM_{SAC}D_P$) versions of this problem are also coNP-complete [5]. The proof consists in a reduction from $M_{SAC}D_P$ to $DFM_{SAC}D_P$ (resp. $NbM_{SAC}D_P$) and the polynomial transformation is based on the one of Proposition 2 (resp. Proposition 3).

B. Interval State Avoidance Control Problem

Proposition 5: I_{SACP} is NP-complete.

Proof: First, we prove that $I_{SACP} \in$ NP. Given $\mathcal{T}$, $\langle \mathcal{D}_{Obs}, M \rangle$, two predicates *Min* and *Max*, we select a controller $\mathcal{C} = \langle \mathcal{S}, E \rangle$ and test that *Min* $\subseteq \mathsf{reach}(\mathcal{T}_{/\mathcal{C}}) \subseteq$ *Max*. This property can be verified in polynomial time. If $\mathcal{C}$ satisfies this property, then it is a solution to I_{SACP}. Therefore, $I_{SACP} \in$ NP.

The second part of the proof consists in a reduction from 3SAT to I_{SACP}. An instance of I_{SACP} is built from 3SAT as follows. The system to control $\mathcal{T}_\phi$ and the set of observations $\langle \mathcal{D}_{Obs}, M \rangle$ are built as in the proof of Proposition 1. We set *Min* $= \{true\}$ and *Max* $= \overline{\{bad\}}$.

Now, we prove the correctness of the polynomial transformation. For that, we show that ϕ is satisfiable iff there exists a controller $\mathcal{C}$ such that *Min* $\subseteq \mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}}) \subseteq$ *Max*. This equivalence is proven as follows:

- If ϕ is not satisfiable, then there is no controller $\mathcal{C}$ such that *Min* $\subseteq \mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}}) \subseteq$ *Max*. Indeed, a controller $\mathcal{C}$ solving I_{SACP} must prevent from reaching bad, because if not, $\mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}}) \not\subseteq$ *Max*. Then, Lemma 4 remains valid, i.e. if ϕ is not satisfiable, then $true$ is not reachable in the system $\mathcal{T}_\phi$ controlled by a valid controller. Thus, there is no controller $\mathcal{C}$ such that *Min* $\subseteq \mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}}) \subseteq$ *Max*.
- If ϕ is satisfiable, then there exists a controller $\mathcal{C}$ such that *Min* $\subseteq \mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}}) \subseteq$ *Max*. Indeed, if ϕ is satisfiable, then the controller $\mathcal{C}_1$ defined in the proof of Lemma 5 is such that $true$ is reachable and bad is not reachable. This controller also satisfies that *Min* $\subseteq \mathsf{reach}((\mathcal{T}_\phi)_{/\mathcal{C}_1}) \subseteq$ *Max*. Thus, there exists at least one controller solving I_{SACP}. ■

The deadlock free (DFI_{SACP}) and non-blocking (NbI_{SACP}) versions of this problem are also NP-complete [5]. The proof consists in a reduction from I_{SACP} to DFI_{SACP} (resp. NbI_{SACP}) and the polynomial transformation is based on the one of Proposition 2 (resp. Proposition 3).

C. Maximal Cardinality State Avoidance Control Problem

Proposition 6: MC_{SACP} is NP-complete.

Proof: First, we prove that $MC_{SACP} \in$ NP. Given $\mathcal{T}$, $\langle \mathcal{D}_{Obs}, M \rangle$, and Bad, we select a controller $\mathcal{C} = \langle \mathcal{S}, E \rangle$ and test that $\mathcal{C}$ is valid and $|\mathsf{reach}(\mathcal{T}_{/\mathcal{C}})| \geq N$. These properties can be verified in polynomial time. If $\mathcal{C}$ satisfies these properties, then it is a solution to MC_{SACP}. Therefore, $MC_{SACP} \in$ NP.

The second part of the proof consists in a reduction from 3SAT to MC_{SACP}. An instance of MC_{SACP} is built from 3SAT as follows. The system to control $\mathcal{T}_\phi$, the set of observations $\langle \mathcal{D}_{Obs}, M \rangle$ and the set Bad are built as in the proof of Proposition 1. We set $N = 3.k + 5$.

Now, we prove the correctness of the polynomial transformation. For that, we show that ϕ is satisfiable iff there exists a valid controller $\mathcal{C}$ such that $|\mathsf{reach}(\mathcal{T}_{/\mathcal{C}})| \geq 3.k + 5$. This equivalence is proven as follows:

- If ϕ is not satisfiable, then there exists no valid controller $\mathcal{C}$ such that $|\mathsf{reach}(\mathcal{T}_{/\mathcal{C}})| \geq 3.k + 5$. Indeed, by Lemma 4, if ϕ is not satisfiable, then a maximal valid controller allows σ^1 in ost and forbids σ^2 in ost. In consequence, all valid controllers $\mathcal{C}$ are such that $|\mathsf{reach}(\mathcal{T}_{/\mathcal{C}})| < 3.k + 5$.
- If ϕ is satisfiable, then there exists a valid controller $\mathcal{C}$ such that $|\mathsf{reach}(\mathcal{T}_{/\mathcal{C}})| \geq 3.k + 5$. Indeed, the controller $\mathcal{C}_1$ defined in the proof of Lemma 5 is valid and such that $|\mathsf{reach}(\mathcal{T}_{/\mathcal{C}})| \geq 3.k + 5$. ■

The deadlock free ($DFMC_{SACP}$) and non-blocking ($NbMC_{SACP}$) versions of this problem are also NP-complete [5]. The proof consists in a reduction from MC_{SACP} to $DFMC_{SACP}$ (resp. $NbMC_{SACP}$) and the polynomial transformation is based on the one of Proposition 2 (resp. Proposition 3).

VI. Conclusion

In this paper, we considered the computational complexity of several problems. We studied the problems consisting in (i) computing a maximal solution for $SACP$, (ii) deciding if a given controller is maximal, (iii) deciding if there exists a solution within a range of behaviors, (iv) deciding whether there exists a valid controller, for which a given minimal number of states is reachable in the resulting controlled system. We proved that no deterministic polynomial algorithm can solve these problems (unless P = NP). These properties hold for deterministic and non-deterministic systems to control and also when the deadlock free or non-blocking properties must be ensured.

A potential approach for future research is to develop *efficient* approximate algorithms using for example the linear programming. Another area for future research is to study sub-cases of the considered problems, where we make assumptions on the problems, to make their computation *easier*.

VII. Acknowledgements

The authors would like to thank Prof. J-F. Raskin and Nicolas Maquet for their helpful insights.

References

[1] C. Cassandras and S. Lafortune. *Introduction to Discrete Event Systems (2nd edition)*. Springer, 2008.

[2] P. Gohari and W. M. Wonham. On the complexity of supervisory control design in the rw framework. *IEEE Transactions on Systems, Man, and Cybernetics, Part B*, 30(5):643–652, 2000.

[3] R.C. Hill, D.M. Tilbury, and S. Lafortune. Covering-based supervisory control of partially observed discrete event systems for state avoidance. In *9th International Workshop on Discrete Event Systems*, May 2008.

[4] G. Kalyon, T. Le Gall, H. Marchand, and T. Massart. Control of infinite symbolic transition sytems under partial observation. *Accepted to European Control Conferences*, 2009.

[5] G. Kalyon, T. Le Gall, H. Marchand, and T. Massart. Results of np-completeness for state-feedback controllers. Technical report of the verification group 121, Université Libre de Bruxelles, March 2009.

[6] R. Kumar, V. Garg, and S.I. Marcus. Predicates and predicate transformers for supervisory control of discrete event dynamical systems. *IEEE Trans. Autom. Control*, 38(2):232–247, 1993.

[7] P.J. Ramadge and W.M. Wonham. The control of discrete event systems. *Proceedings of the IEEE; Special issue on Dynamics of Discrete Event Systems*, 77(1):81–98, 1989.

[8] K. Rudie and J. C. Willems. The computational complexity of decentralized discrete-event control problems. *IEEE Transactions on Automatic Control*, 40:1313–1319, 1995.

[9] S. Takai and S. Kodama. Characterization of all m-controllable subpredicates of a given predicate. *International Journal of Control*, 70:541–549(9), 10 July 1998.

[10] J. N. Tsitsiklis. On the control of discrete event dynamical systems. *Mathematics of Control, Signals and Systems*, 2(2):95–107, 1989.

[11] W.M. Wonham. Lecture notes on control of discrete-event systems. Technical report, University of Toronto, 2005.

[12] W.M. Wonham and P.J. Ramadge. Modular supervisory control of discret-event systems. *Mathematics of Control, Signals, and Systems*, 1(1):13–30, 1988.