

Supervisory Controller Synthesis for Non-terminating Processes is an Obliging Game

Rupak Majumdar and Anne-Kathrin Schmuck

Abstract—We present a new algorithm to solve the supervisory control problem over non-terminating processes modeled as ω -regular automata. A solution to the problem was obtained by Thistle in 1995 which uses complex manipulations of automata. This algorithm is notoriously hard to understand and, to the best of our knowledge, has never been implemented. We show a new solution to the problem through a reduction to reactive synthesis.

A naive, and incorrect, approach reduces the supervisory control problem to a reactive synthesis problem that asks for a control strategy which ensures the given specification if the plant behaves in accordance to its liveness properties. This is insufficient. A correct control strategy might not fulfill the specification but force the plant to invalidate its liveness property. To prevent such solutions, supervisory control additionally requires that the controlled system is *non-conflicting*: any finite word compliant with the supervisor should be extendable to a word satisfying the plants' liveness properties.

To capture this additional requirement, our solution goes through *obliging games* instead. An obliging game has two requirements: a *strong* winning condition as in reactive synthesis and a *weak* winning condition. A strategy is winning if it satisfies the strong condition and additionally, every partial play can be extended to satisfy the weak condition. Obliging games can be reduced to ω -regular reactive synthesis, for which symbolic algorithms exist. We reduce supervisor synthesis to obliging games. The strong condition is an implication: if the plant behaves in accordance with its liveness properties, the specification should also hold. The weak condition is the plants' liveness property.

The reduction to obliging games gives a conceptually simple algorithm for supervisor synthesis over non-terminating processes. Moreover, it allows symbolic implementations of the involved constructions using symbolic tools from reactive synthesis.

I. INTRODUCTION

Supervisory control theory (SCT) is a branch of control theory which is concerned with the control of discrete-event dynamical systems with respect to temporal specifications. Given such a system, SCT asks to synthesize a *supervisor* that restricts the possible sequences of events such that any remaining sequence fulfills a given specification. The field of SCT was established by the seminal work of Ramadge and Wonham [1] concerning the control of *terminating processes*, i.e., systems whose behavior can be modeled by regular languages over finite words. This setting is well understood and summarized in standard text books [2], [3].

Already 30 years ago, Thistle and Wonham extended the scope of SCT to *non-terminating processes* [6], i.e., to the supervision of systems whose behavior can be modeled by regular languages over *infinite* words. Non-terminating processes naturally occur in models of infinitely executing reactive

systems; ω -words allow convenient modeling of liveness specifications for such systems. In a sequence of papers [6]–[8] culminating in [9], Thistle and Wonham laid out the foundations for supervisory control theory over non-terminating processes and showed, in particular, symbolic algorithms to synthesize supervisors for general ω -regular specifications under general ω -regular plant liveness properties. A key observation was the relationship between SCT and Church's problem from logic [10], and hence to techniques from reactive synthesis.

Unfortunately, the algorithms given in these papers to solve this supervisory control problem remain notoriously difficult to understand. The symbolic algorithm in [9], which solves the problem in the most general setting, involves an intricate fixed point computation over the ω -regular languages, using structural operations on finite-state automata representations. As a direct result of this complexity, to the best of our knowledge, supervisor synthesis for non-terminating processes has never been implemented and there are very few results building on top of the results of Thistle and Wonham.

In this paper, we show an alternate proof of supervisor synthesis for non-terminating processes that relates the problem to reactive synthesis for ω -regular specifications. Unlike the complex manipulations of Thistle's paper, our proof is conceptually very simple, and reduces the problem to a class of reactive synthesis problems, called *obliging games*.

While connections between reactive synthesis and SCT are well-known, (see, e.g., the recent surveys [11] and [12] connecting the two fields), the reduction of supervisor synthesis to reactive synthesis is not obvious. To understand the source of difficulty, let us recall the setting of the problem. We are given an automaton that forms the “arena” for the synthesis problem, and we are given *two* ω -regular languages defined on this automaton. The first language (let's call it A) models *liveness assumptions* on the plant: a supervisor can assume that the (uncontrolled) plant language will satisfy this assumption. The second language (call it S) provides the specification that the supervisor must uphold whenever the plant operates in accordance to its liveness properties (i.e., if the assumption holds), by preventing certain controllable events over time.

One can easily transform the automaton to a two-player game, as in reactive synthesis, and naively ask for a winning strategy for the winning condition $A \Rightarrow S$, which states that if the plant satisfies its assumption, then the resulting behavior satisfies the specification. While this reduction seems natural, it is incorrect in the context of SCT.¹

¹ We point out that there exist papers on reactive synthesis which make tangential comments on solving SCT for non-terminating processes based, we believe, on this reduction, see e.g., [13, p.18].

The problem is that a control strategy may “cheat” and enforce the above implication vacuously by actively preventing the plant from satisfying its liveness properties. In SCT, such undesired solutions are ruled out by a *non-conflicting* requirement: any finite word compliant with the supervisor must be extendable to an infinite word that satisfies A . Hence, a non-conflicting supervisor always allows the plant to fulfill its liveness property. The non-conflicting requirement is not a linear property [11], and cannot be “compiled away” in reactive synthesis.

The main contribution of this paper is a reduction of the supervisory control problem to a class of reactive synthesis problems called *obliging games* [14] that precisely capture a notion of non-conflicting strategies in the context of reactive synthesis. The main result of [14] shows that obliging games can be reduced to usual reactive synthesis on a larger game. Once the intuitive connection between supervisory control and obliging games is made, the formal reduction is almost trivial. We consider this simplicity as a *feature* of our proof: the conceptual reduction from supervisory control to obliging games, and hence to reactive synthesis, forms a separation of concerns between (a) the modeling of specifications and non-conflicting strategies and (b) the (non-trivial, but well-understood) algorithmics of solving games. (The complexity of Thistle’s algorithm is that it implicitly combines both steps into one algorithm.) Moreover, the reduction gives—in principle—a symbolic implementation of supervisory controller synthesis for non-terminating processes and arbitrary ω -regular plant liveness properties and specifications, based on symbolic implementations of reactive synthesis.

Other Related Work This paper continues recent efforts in establishing a formal connection between reactive synthesis and SCT for *terminating processes* [11], [15], [16] and *non-terminating processes* [12]. While [12] focusses on a language-theoretic connection, this paper establishes a connection between synthesis algorithms over automata realizations.

Within the SCT community, non-terminating processes have gained more and more attention in recent years. They have, for example, been considered for using different specification languages such as linear temporal logic (LTL) [17], computational tree logic (CTL) [18], epistemic temporal logic [19], or modal logic [20]. Further, within abstraction-based controller design the resulting abstractions are typically non-terminating, motivating the use of these procedures, as, e.g., in [21]. However, within all the listed work, the plant itself does not possess non-trivial liveness properties, which allows to transform the resulting synthesis problem to the usual setting of reactive synthesis. Notable exceptions are, e.g., [22], [23]. Here, existing synthesis tools are restricted to *deterministic* Büchi automata models, which only capture a strict subclass of ω -regular properties.

Symbolic algorithms for GR(1) specifications satisfying a non-conflicting requirement were presented in [24]. Their algorithm has the advantage of a “direct” implementation using symbolic manipulation of sets of states. We leave as future work whether a similar direct algorithm can be designed for general obliging games.

II. PRELIMINARIES

Formal Languages. Given a finite alphabet Σ , we write Σ^* , Σ^+ , and Σ^ω for the sets of finite words, non-empty finite words, and infinite words over Σ , and write $\Sigma^\infty = \Sigma^* \cup \Sigma^\omega$. We write $w \leq v$ (resp., $w < v$) if w is a prefix of v (resp., a strict prefix of v). The set of all prefixes of a word $w \in \Sigma^\omega$ is denoted $\text{pfx}(w) \subseteq \Sigma^*$. For $L \subseteq \Sigma^*$, we have $L \subseteq \text{pfx}(L)$. A language L is *prefix-closed* if $L = \text{pfx}(L)$. The *limit* $\lim(L)$ of $L \subseteq \Sigma^*$ contains all words $\alpha \in \Sigma^\omega$ which have infinitely many prefixes in L and we define $\text{clo}(\mathcal{L}) := \lim(\text{pfx}(\mathcal{L}))$ as the *topological closure* of $\mathcal{L} \subseteq \Sigma^\omega$.

Automata. An automaton is a tuple $M = (X, \Sigma, \delta, q_0)$, with state set X , alphabet Σ , initial state $q_0 \in X$, and the partial transition function $\delta : X \times \Sigma \rightarrow 2^X$. For $x \in X$ and $\sigma \in \Sigma$, we write $\delta(x, \sigma)!$ to signify that $\delta(x, \sigma)$ is defined. We call M *deterministic* if $\delta(x, \sigma)!$ implies $|\delta(x, \sigma)| = 1$. We call M *non-blocking* if for all $x \in X$ there exists at least one $\sigma \in \Sigma$ s.t. $\delta(x, \sigma)!$.

A *path* of M is a finite or infinite sequence $\pi = x_0 x_1 \dots$ s.t. for all $k \in \text{Length}(\pi) - 1$ there exists some $\sigma_k \in \Sigma$ s.t. $x_{k+1} \in \delta(x_k, \sigma_k)$. If π is finite, we denote by $\text{Last}(\pi) = x_n$ its last element. We collect all finite and infinite paths of the automaton M in the sets $P(M) \subseteq X^*$ and $\mathcal{P}(M) \subseteq X^\omega$, respectively. Given a string $s = \sigma_0 \sigma_1 \dots \in \Sigma^\infty$ we say that a path π of M is *compliant* with s if $\text{Length}(s) = \text{Length}(\pi) - 1$ and for all $k \in \text{Length}(\pi) - 1$ we have $x_{k+1} \in \delta(x_k, \sigma_k)$. We define by $\text{Paths}_M(s)$ the set of all paths of M compliant with s . We collect all finite and infinite strings that are compliant with M in the sets $L(M) := \{s \in \Sigma^* \mid \text{Paths}_M(s) \neq \emptyset\}$ and $\mathcal{L}(M) := \{s \in \Sigma^\omega \mid \text{Paths}_M(s) \neq \emptyset\}$, respectively. If M is non-blocking, we have $\text{pfx}(\mathcal{L}(M)) = L(M)$. If M is deterministic we have $|\text{Paths}_M(s)| = 1$ for all $s \in L(M)$.

Acceptance Conditions. We consider acceptance conditions defined over sets of states of a given automaton M . For a path π , define $\text{Inf}(\pi) = \{x \in X \mid x_k = x \text{ for infinitely many } k \in \mathbb{N}\}$ to be the set of states visited infinitely often along π .

Let $F \subseteq X$ be a subset of states. We say that an *infinite* string $s \in \Sigma^\omega$ satisfies the *Büchi condition* $\mathcal{F}^B = \{F\}$ on M if there exists a path $\pi \in \text{Paths}_M(s)$ such that $\text{Inf}(\pi) \cap F \neq \emptyset$.

Let $\mathcal{F} = \{\langle G_1, R_1 \rangle, \dots, \langle G_m, R_m \rangle\}$ be a set, where each $G_i, R_i \subseteq X$, $i = 1, \dots, m$, is a subset of states. We say that a string $s \in \Sigma^\omega$ satisfies the *Rabin condition* $\mathcal{F}^R = \mathcal{F}$ on M if there exists a path $\pi \in \text{Paths}_M(s)$ such that $\text{Inf}(\pi) \cap G_i \neq \emptyset$ and $\text{Inf}(\pi) \cap R_i = \emptyset$ for some $i \in [1; m]$. It satisfies the *Streett condition* $\mathcal{F}^S = \mathcal{F}$ if $\text{Inf}(\pi) \cap G_i = \emptyset$ or $\text{Inf}(\pi) \cap R_i \neq \emptyset$ for all $i \in [1; m]$. Rabin and Streett conditions are *duals*, i.e., if π satisfies the Rabin condition \mathcal{F}^R it violates the equivalent Streett condition $\mathcal{F}^S = \mathcal{F}^R$.

We call an automaton equipped with a Büchi, Rabin or Streett acceptance condition a Büchi, Rabin or Streett automaton, respectively. We collect all infinite strings (resp. paths) satisfying the specified acceptance condition \mathcal{F} over M , in the accepted language $\mathcal{L}(M, \mathcal{F}) \subseteq \Sigma^\omega$ (resp. in the set $\mathcal{P}(M, \mathcal{F}) \subseteq X^\omega$). We remark that *deterministic* Rabin and Streett automata as well as *non-deterministic* Büchi automata can realize any ω -regular language $\mathcal{L} \subseteq \Sigma^\omega$. This is not true for *deterministic* Büchi automata which are less expressive.

III. THE SUPERVISOR SYNTHESIS PROBLEM

We define the supervisory controller synthesis problem following the original formulation for $*$ -languages [1] and the subsequent extension to ω -languages in [6]–[9].

A. Problem Statement

Let Σ be a finite alphabet of *events* partitioned into controllable events Σ_c and uncontrollable events Σ_{uc} , that is, $\Sigma = \Sigma_c \dot{\cup} \Sigma_{uc}$. A *plant* is a tuple (L_P, \mathcal{L}_P) , where $L_P \subseteq \Sigma^*$ is a prefix-closed $*$ -language and $\mathcal{L}_P \subseteq \Sigma^\omega$ is an ω -language. A *specification* is an ω -language $\mathcal{L}_S \subseteq \Sigma^\omega$.

Intuitively, L_P models all possible event sequences the plant can generate, while \mathcal{L}_P is a liveness assumption on the plant behavior, which distinguishes a set of infinite event sequences. The languages L_P and \mathcal{L}_P play the role of the *unmarked* and *marked* plant language of the original Ramadge and Wonham framework [1], where \mathcal{L}_P and \mathcal{L}_S are non-prefix closed $*$ -languages, rather than ω -languages. The plant represents the (external) behavior of the process to be controlled, and the specification restricts the behavior of the plant to a set of desired behaviors. The set Σ_c denotes all events the controller can prevent the plant from executing, while the set Σ_{uc} denotes events that cannot be prevented by the controller.

A *control pattern* γ is a subset of Σ containing Σ_{uc} . We collect all control pattern in the set $\Gamma := \{\gamma \subseteq \Sigma \mid \Sigma_{uc} \subseteq \gamma\}$. A *supervisor* is a map $f : \Sigma^* \rightarrow \Gamma$ that maps each (finite) past event sequence $s \in \Sigma^*$ to a control pattern $f(s) \in \Gamma$. The control pattern specifies the set of enabled successor events after the occurrence of s , the definition of control patterns ensures that uncontrollable events are always enabled. A word $s \in \Sigma^*$ is called *consistent* with f if for all $\sigma \in \Sigma$ and $t\sigma \in \text{pfx}(s)$, it holds that $\sigma \in f(t)$. We write L_f for the set of all words consistent with f and define $\mathcal{L}_f := \lim(L_f)$.

With these definitions, the supervisor synthesis problem can be formally stated as follows.

Problem 1 (Language-Theoretic Supervisor Synthesis). Given an alphabet $\Sigma = \Sigma_c \dot{\cup} \Sigma_{uc}$, a plant model (L_P, \mathcal{L}_P) , where $L_P \subseteq \Sigma^*$ and $\mathcal{L}_P \subseteq \Sigma^\omega$, and a specification $\mathcal{L}_S \subseteq \Sigma^\omega$, synthesize, if possible, a supervisor $f : \Sigma^* \rightarrow \Gamma$ s.t.

- (i) the closed-loop satisfies the specification, i.e.,

$$\emptyset \subsetneq \mathcal{L}_f \cap \mathcal{L}_P \subseteq \mathcal{L}_S \quad (1a)$$

- (ii) the plant and the supervisor are *non-conflicting*, i.e.,

$$L_f \cap L_P \subseteq \text{pfx}(\mathcal{L}_f \cap \mathcal{L}_P), \quad (1b)$$

or determine that no such supervisor exists. A supervisor f is a solution to the supervisor synthesis problem over $((L_P, \mathcal{L}_P), \mathcal{L}_S)$ if it satisfies (1a) and (1b). \triangleleft

The constraint (1b) ensures that the plant is always able to generate events allowed by f s.t. it generates a word in its marked language \mathcal{L}_P . Then, by (1a), all such generated words must be contained in the specification \mathcal{L}_S .

B. Automata Representations for Supervisor Synthesis

We now turn to effective algorithms for supervisor synthesis when the plant and specification languages are accepted by

automata over finite or infinite words. In fact, we shall assume the input to the supervisory synthesis problem will be given as an automaton as described in the following definition.

Definition III.1. Let $M = (X, \Sigma, \delta, q_0)$ be an automaton with the following properties: (a) M is deterministic, and (b) distinct transitions in M carry distinct labels, i.e. for any $\sigma, \sigma' \in \Sigma$ and $x \in X$ we have that $\delta(x, \sigma) = \delta(x, \sigma')$ implies $\sigma = \sigma'$. Further, let \mathcal{F}_P^S and \mathcal{F}_S^R be a Streett and a Rabin condition over M , respectively. Then we call the tuple $(M, \mathcal{F}_P^S, \mathcal{F}_S^R)$ a *Streett/Rabin supervisor synthesis automaton*.

Note that the assumptions on the automaton M in Def. III.1 are without loss of generality. Any ω -regular language can be accepted by a deterministic Streett or Rabin automaton. Further, an automaton with non-distinct labels can be modified by extending the state space X to $X \times \Sigma$ to fulfill this property.

Remark 1. We do not assume that M is *full* or *non-blocking*. In supervisory control theory M is assumed to model the actual capabilities of an (already existing) system and thereby realizes L_P . It should be noted that completing M or deleting blocking states might change the supervisor synthesis problem at hand, due to the special treatment of uncontrollable events.

C. State-Based Supervisor Synthesis

We now formulate an equivalent version of Problem 1 in terms of M and *state-based* supervisors. A *state-based supervisor* is a map $\check{f} : P(M) \rightarrow \Gamma$. A path π over M is called *consistent* with \check{f} if for all $x, x' \in X$ and $\nu xx' \in \text{pfx}(\pi)$, there exists an event $\sigma \in \check{f}(\nu x)$ s.t. $x' = \delta(x, \sigma)$. Let $P(M, \check{f})$ be the set of all paths of M consistent with \check{f} and define $\mathcal{P}(M, \check{f}) := \lim(P(M, \check{f}))$. We can now re-state Problem 1 into the following state-based supervisor synthesis problem.

Problem 2 (State-based Supervision). Given a Streett/Rabin supervisor synthesis automaton $(M, \mathcal{F}_P^S, \mathcal{F}_S^R)$, synthesize, if possible, a state-based supervisor $\check{f} : P(M) \rightarrow \Gamma$ s.t.

$$\emptyset \subsetneq \mathcal{P}(M, \check{f}) \cap \mathcal{P}(M, \mathcal{F}_P^S) \subseteq \mathcal{P}(M, \mathcal{F}_S^R), \text{ and} \quad (2a)$$

$$P(M, \check{f}) \subseteq \text{pfx}(\mathcal{P}(M, \check{f}) \cap \mathcal{P}(M, \mathcal{F}_P^S)), \quad (2b)$$

or determine that no such supervisor exists. A state-based supervisor \check{f} is a solution to the supervisor synthesis problem over $(M, \mathcal{F}_P^S, \mathcal{F}_S^R)$ if it satisfies (2a) and (2b).

The structure of the automaton M ensures that there is a one-to-one correspondence between a word in $L_P = L(M)$ and its unique path $\pi = \text{Paths}_M(s)$ over M . Further, as transition labels are unique in M (see Def. III.1 (b)), there is also a unique word s associated with a path π over M . With these observations, it is easy to show that Problem 1 and Problem 2 are indeed equivalent, as summarized by Thm. III.1 below and proved in App. A.

Theorem III.1. Let $(M, \mathcal{F}_P^S, \mathcal{F}_S^R)$ be a Streett/Rabin supervisor synthesis automaton as in Def. III.1 s.t. $L_P := \mathcal{L}(M)$, $\mathcal{L}_P := \mathcal{L}(M, \mathcal{F}_P^S)$ and $\mathcal{L}_S := \mathcal{L}(M, \mathcal{F}_S^R)$. Further, let $f : \Sigma^* \rightarrow \Gamma$ and $\check{f} : P(M) \rightarrow \Gamma$ be an event- and a state-based supervisor, respectively, s.t.

$$\forall s \in L(M) . f(s) = \check{f}(\text{Paths}_M(s)). \quad (3)$$

Then f is a solution to the supervisor synthesis problem over $((L_P, \mathcal{L}_P), \mathcal{L}_P)$ iff \tilde{f} is a solution to the supervisor synthesis problem over $(M, \mathcal{F}_P^S, \mathcal{F}_S^R)$.

Remark 2. Algorithms solving various versions of Problem 2 are studied by Thistle and Wonham in [6]–[9]. All of them are initialized with a deterministic finite-state automaton M equipped with two acceptance conditions \mathcal{F}_P and \mathcal{F}_S where \mathcal{F}_S is a Rabin condition. However, \mathcal{F}_P is chosen to be trivial in [6] (i.e., $\mathcal{L}_P = \Sigma^\omega$), a deterministic Büchi condition in [7], [8], and a deterministic Streett condition in [9]. Since deterministic Büchi automata are strictly less expressive than deterministic Streett automata, and the latter can realize any ω -regular property, we see that the setting of [9], as well as the setting of our paper, defines the most general synthesis procedure for ω -regular plant and specification languages.

It is not directly obvious that Problem 1 is equivalent to the problem studied by Thistle in [9]. In [9] the second clause in Problem 1 is slightly modified to $L_f \cap L_P \subseteq \text{pfx}(\mathcal{L}_f \cap \mathcal{L}_S)$, i.e., the intersection with \mathcal{L}_P on the right of (1b) has changed to \mathcal{L}_S . The condition in [9] obviously implies (1b) if $\mathcal{L}_S \subseteq \mathcal{L}_P$. Further, pre-processing \mathcal{L}_S to $\mathcal{L}_S \cap \mathcal{L}_P$ does not change the statement of claim (i) in Problem 1 and is therefore without loss of generality. The algorithmic procedure given in [9] therefore implicitly requires $\mathcal{L}_S \subseteq \mathcal{L}_P$ or a pre-processing step ensuring this by re-defining \mathcal{L}_S to $\mathcal{L}_S \cap \mathcal{L}_P$.

D. Example

Consider the synthesis automaton M depicted in Fig. 1 for a state-based supervisor synthesis problem. Here, the alphabet is $\Sigma = \{a, b, c\}$, partitioned in $\Sigma_c = \{a, b\}$ (indicated by a tick on the corresponding edges in Fig. 1) and $\Sigma_{uc} = \{c\}$. The plants' liveness property assumes that the plant visits the state p_2 always again. This is specified by a Büchi acceptance condition $\mathcal{F}_P^B = \{p_2\}$, and indicated by the light-blue double circle around state p_2 in Fig. 1. The Büchi condition \mathcal{F}_P^B can be equivalently formulated as the Streett condition $\mathcal{F}_P^S = \{(\{p_1, p_2, p_3\}, \{p_1\})\}$. The light-blue “plant marking” on M models that any trace of the *uncontrolled* system will visit p_2 always again. The specification is given by a Büchi condition with $\mathcal{F}_S^B = \{p_1\}$, indicated by the red double circle around p_1 in Fig. 1. Again, we can equivalently represent \mathcal{F}_S^B as the Rabin condition $\mathcal{F}_S^R = \{(\{p_2\}, \emptyset)\}$. The red “specification marking” implies that the supervisor must ensure that the controlled system visits the state p_1 infinitely often. The supervisor can only disable controllable actions; thus, every control pattern allows c .

The supervisor synthesis problem asks, given $(M, \mathcal{F}_P^S, \mathcal{F}_S^R)$, to synthesize a state-based supervisor that ensures (i) all traces in the controlled system which fulfill the plant's liveness assumption also fulfill the specification (i.e., whenever p_2 is always visited again, also p_1 is always visited again), and that (ii) the plant under control is always able to fulfill its liveness property (i.e., the controller does not prevent the plant from visiting p_2 again in the future).

A state-based supervisor solving this problem is given by the following rule: any path ending in p_0 is mapped to $\{a, c\}$, any path ending in p_1 is mapped to $\{b, c\}$, and any path ending in

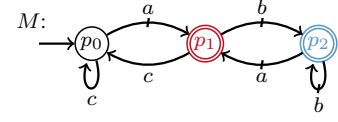


Fig. 1. Synthesis automaton M for example in Sec. III-D. Plant and specification markings indicated in blue (p_2) and red (p_1), respectively. Controllable events $\{a, b\}$ indicated by a ticked transition. Event c is uncontrollable.

p_2 is mapped to $\{a, c\}$. This effectively disables the self-loop on event b in state p_2 . Note that this solution is not unique: for each $n \geq 0$, a supervisor could map paths ending in p_0 and p_1 as before, but map paths ending in p_2 to $\{a, b, c\}$ if the number of visits to p_2 is less than n and to $\{a, c\}$ otherwise. In this case, the supervisor would allow the self loop on b in p_2 to be taken n number of times.

Remark 3. The above example demonstrates the well-known fact that for ω -languages, there may not exist a *maximally permissive* supervisor, i.e., a supervisor f solving Problem 1 s.t. $\mathcal{L}_{f'} \cap \mathcal{L}_P \subseteq \mathcal{L}_f \cap \mathcal{L}_P$ for all other supervisors f' solving Problem 1. In the above example, the maximal permissive supervisor would need to “eventually” disable b which cannot be modeled by a supervisor mapping from *finite* past strings to control patterns. This situation is in contrast to supervisor synthesis for $*$ -languages where maximally permissive solutions to Problem 1 always exist.

IV. FROM SUPERVISOR SYNTHESIS TO GAMES

We shall reduce Problem 2 to solving a class of two-player games on graphs with ω -regular winning conditions.

A. Two-Player Games

A *two-player game graph* $G = (Q^0, Q^1, \delta^0, \delta^1, q_{init})$ consists of two finite disjoint state sets Q^0 and Q^1 , two transition functions $\delta^0 : Q^0 \rightarrow 2^{Q^1}$ and $\delta^1 : Q^1 \rightarrow 2^{Q^0}$, and an initial state $q_{init} \in Q^0$. We write $Q = Q^0 \cup Q^1$.

Given a game graph G , a *strategy* for player 0 is a function $h : q_{init}(Q^1 Q^0)^* \rightarrow Q^1$; it is *memoryless* if $h(\nu q^0) = h(q^0)$ for all $\nu \in (Q^0 Q^1)^*$ and all $q^0 \in Q^0$. A *strategy* $g : q_{init}(Q^1 Q^0)^* Q^1 \rightarrow Q^0$ for player 1 is defined analogously. The sequence $\rho \in Q^\infty$ is called a *play* over G if $\rho(0) = q_{init}$ and for all $k \in \text{Length}(\rho) - 1$, we have $\rho(k+1) \in \delta^0(\rho(k))$ if $\text{Last}(\rho) \in Q^0$ and $\rho(k+1) \in \delta^1(\rho(k))$ otherwise. The play ρ is *compliant* with h and/or g if additionally $h(\rho|_{[0,k]}) = \rho(k+1)$ if $\text{Last}(\rho) \in Q^0$ and/or $g(\rho|_{[0,k]}) = \rho(k+1)$ if $\text{Last}(\rho) \in Q^1$. We denote by $P(G, h)$ and $\mathcal{P}(G, h)$ the set of finite and infinite plays over G compliant with h .

We define ω -regular winning conditions for two-player games. These are specified analogously to acceptance conditions for automata over subsets of states Q . That is, we consider Büchi, Rabin and Streett conditions \mathcal{F} as defined in Sec. II over subsets of Q and say that a play ρ is winning w.r.t. \mathcal{F} if ρ satisfies \mathcal{F} on G . In addition, we also consider the *parity* accepting condition [27]. For the parity condition with k parities, we assume there is a coloring function $\Omega : Q \rightarrow \{0, \dots, k-1\}$. A play ρ is winning if the maximum color seen infinitely often is even.

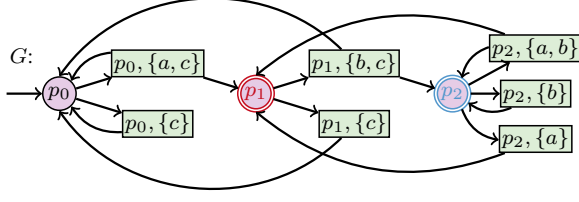


Fig. 2. Game graph $G(M)$ associated with the synthesis automaton M in Fig. 1. Supervisor and plant player states are indicated by a circular violet and a rectangular green shape, respectively. Rectangular states (p, γ) indicate the control pattern γ chosen by the supervisor in state p of M .

We call a game graph equipped with a Büchi, Rabin, Streett, or parity winning condition \mathcal{F} a Büchi, Rabin, Streett, or parity game, respectively, and denote it by the tuple (G, \mathcal{F}) . The set of all winning plays over G w.r.t. \mathcal{F} is denoted $\mathcal{P}(G, \mathcal{F})$. A strategy h is *winning* in a game (G, \mathcal{F}) , if $\mathcal{P}(G, h) \subseteq \mathcal{P}(G, \mathcal{F})$.

We recall the following well known theorem [25]–[28].

Theorem IV.1 (ω -regular games). *It is decidable if player 0 has a winning strategy in a two-player game with a winning condition given by a Büchi, Rabin, Streett, or parity acceptance condition.*

B. Supervisor Synthesis as a Two-Player Game

Intuitively, one can interpret the interaction of a supervisor with the plant as a two-player game over M . Player 0 (the supervisor) picks a control pattern $\gamma \in \Gamma$ and player 1 (the plant) resolves the remaining non-determinism by choosing a transition allowed by γ . We formalize the construction below.

Definition IV.1. Let $M = (X, \Sigma, \delta, q_0)$ be as in Def. III.1 with $\Sigma_{uc} \subseteq \Sigma$ and $\Gamma := \{\gamma \subseteq \Sigma \mid \Sigma_{uc} \subseteq \gamma\}$. Then we define its associated game graph as $G(M) = (Q^0, Q^1, \delta^0, \delta^1, q_0)$ s.t.

- $Q^0 = X$
- $Q^1 = X \times \Gamma$
- $\delta^0(x) = \{x\} \times \Gamma$
- $x' \in \delta^1((x, \gamma))$ iff $\sigma \in \gamma$ and $x' = \delta(x, \sigma)$.

Intuitively, the game graph G makes the choice of the control pattern taken by the state-based supervisor over M explicit by inserting player 1 states in between any two player 0 states. I.e., the choice of control pattern γ in state $x \in X$ of M corresponds to the move of player 0 from $q = x$ to $q' = (x, \gamma)$ in G . Further, as M is assumed to have unique transition labels, this expansion allows to remove all transition labels resulting in an unlabeled game graph G as defined in Sec. IV-A. Fig. 2 shows the two-player game graph $G(M)$ corresponding to M in Fig. 1.

We now discuss an appropriate winning condition for the game. Consider the state-based supervisor synthesis problem (Problem 2) over the Streett/Rabin supervisor synthesis automaton $(M, \mathcal{F}_P^S, \mathcal{F}_S^R)$. Here, (2a) requires that any infinite trace over M which is both compliant with f and fulfills the plant assumption \mathcal{L}_P also fulfills the specification \mathcal{L}_S . Hence, we can equivalently write (2a) as the implication

$$\forall \pi \in \mathcal{P}(M, \check{f}) . (\pi \in \mathcal{P}(M, \mathcal{F}_P^S) \Rightarrow \pi \in \mathcal{P}(M, \mathcal{F}_S^R)), \quad (4)$$

³We restrict depicted control patterns to events enabled at the source state.

which is in turn equivalent to

$$\forall \pi \in \mathcal{P}(M, \check{f}) . (\pi \notin \mathcal{P}(M, \mathcal{F}_P^S) \vee \pi \in \mathcal{P}(M, \mathcal{F}_S^R)). \quad (5)$$

Consequently, (2a) is achieved by a supervisor \check{f} which ensures plays over M either *do not* satisfy the Streett condition \mathcal{F}_P^S or fulfill the Rabin condition \mathcal{F}_S^R . However, as Rabin and Streett conditions are duals, *not satisfying* the Streett condition \mathcal{F}_P^S is equivalent to *satisfying* the Rabin condition $\mathcal{F}_P^R := \mathcal{F}_P^S$. Further, given the definition of Rabin winning conditions (see Sec. II), it is easy to see that a path over M satisfies either the Rabin condition \mathcal{F}_P^R or the Rabin condition \mathcal{F}_S^R iff it satisfies the Rabin condition $\mathcal{F}_{P \rightarrow S}^R = \mathcal{F}_P^R \cup \mathcal{F}_S^R$. With this observation, we can further rewrite (2a) into the equivalent formula

$$\mathcal{P}(M, \check{f}) \subseteq \mathcal{P}(M, \mathcal{F}_{P \rightarrow S}^R). \quad (6)$$

Thus, an obvious choice for the winning condition over the game graph $G(M)$ is the Rabin condition $\mathcal{F}_{P \rightarrow S}^R$.

Example IV.1. Consider the example from Sec. III-D and recall that $\mathcal{F}_P^S = \{(\{p_1, p_2, p_3\}, \{p_1\})\}$ and $\mathcal{F}_S^R = \{(\{p_2\}, \emptyset)\}$. This gives the Rabin winning condition

$$\mathcal{F}_{P \rightarrow S}^R = \{(\{p_1, p_2, p_3\}, \{p_1\}), (\{p_2\}, \emptyset)\} \quad (7)$$

for the induced game over $G(M)$. Intuitively, the condition in (7) states that either p_1 is only visited *finitely often* (first Rabin pair) or p_2 is visited *infinitely often* (second Rabin pair). These two options correspond to either preventing the plant to fulfill its liveness properties (e.g. by always disabling a and b in any state) or to fulfill the specification (e.g. by choosing the strategy given in Sec. III-D). \triangleleft

As the above example demonstrates, a winning strategy for $\mathcal{F}_{P \rightarrow S}^R$ may not fulfill condition (2b). A strategy can choose to satisfy (7) vacuously, by actively preventing the plant to fulfill its liveness properties. Thus, we need to modify the winning condition to ensure the resulting strategy satisfies both (2a) and (2b). As the non-conflicting requirement of (2b) is not a linear property [11], it cannot be easily “compiled away” in reactive synthesis. Therefore, we consider a different type of games instead, called *obliging games*.

V. SUPERVISOR SYNTHESIS VIA OBLIGING GAMES

A. Obliging Games

An obliging game [14] is a triple $(G, \mathcal{S}, \mathcal{W})$ where G is a game graph and \mathcal{S} and \mathcal{W} are two winning conditions, called strong and weak, respectively. To win an obliging game, player 0 (the “controller”) needs to *ensure* the strong winning condition \mathcal{S} against any strategy of player 1 (the “system”), while *allowing* the system to cooperate with him to *additionally* fulfill \mathcal{W} . Such winning strategies are therefore called *gracious* and the synthesis problem for obliging games asks to synthesize such a gracious control strategy or determine that none exists, as formalized in the following problem statement.

Problem 3 (Obliging Games Decision Problem). Given an obliging game $(G, \mathcal{S}, \mathcal{W})$, synthesize a strategy h for player 0 s.t.

- (i) every play over G compliant with h is winning w.r.t. \mathcal{S} , i.e.,

$$\mathcal{P}(G, h) \subseteq \mathcal{P}(G, \mathcal{S}) \quad (8a)$$

- (ii) for every finite play ν over G compliant with h , there exists an infinite play ρ over G compliant with h and winning w.r.t. \mathcal{W} , s.t. $\nu \in \text{pfx}(\rho)$, i.e.,

$$\mathcal{P}(G, h) \subseteq \text{pfx}(\mathcal{P}(G, h) \cap \mathcal{P}(G, \mathcal{W})), \quad (8b)$$

or determine that no such strategy exists.

The following theorem characterizes the solution of Problem 3. It is a direct consequence of the results in [14], [26] and [27], as outlined in App. B.

Theorem V.1. *Every obliging game $(G, \mathcal{S}, \mathcal{W})$ is reducible to a two-player game with an ω -regular winning condition. In particular, an obliging game $(G, \mathcal{F}^R, \mathcal{F}^S)$ with n states, a Rabin condition \mathcal{F}^R with k pairs, and a Streett condition \mathcal{F}^S with l pairs can be reduced to a two-player game with $nk^2k!2^{O(l)}$ states, a parity condition with $= 2k + 2$ parities, and $2k2^{O(l)}$ memory.*

Thus, Thm. IV.1 and Thm. V.1 together imply that obliging games are decidable and one can effectively construct winning strategies of player 0 in such games.

B. Winning Conditions for Supervisor Synthesis

We reduce the supervisor synthesis problem to obliging games. Referring to (8a) in Problem 3, we see that an obvious choice for \mathcal{S} is the Rabin condition $\mathcal{F}_{P \rightarrow S}^R$.

The weak condition is used to rule out strategies or supervisors that ensure the strong condition by falsifying the assumption \mathcal{F}_P^S . Both the non-conflicting requirement in supervisor synthesis and the weak condition in obliging games require that, in every instance of the play, the strategy or the supervisor allows the plant to play in a way that the plant specification (respectively, the weak condition) is satisfied. Consequently, an obvious choice for the weak winning condition in the resulting obliging game is $\mathcal{W} := \mathcal{F}_P^S$.

We can see by inspection that after replacing (2a) by (6) in Problem 2 and defining $\mathcal{S} := \mathcal{F}_{P \rightarrow S}^R$ and $\mathcal{W} := \mathcal{F}_P^S$ in Problem 3, the two problem descriptions match. However, the system models and the corresponding control mechanisms are still different. We therefore need to match state-based supervisors for M with player 0 strategies over $G(M)$, which is formalized in the next subsection.

C. Formal Reduction

Given the reduction from M to a game graph $G(M)$, and the strong and weak winning conditions, it remains to show that the resulting obliging game is indeed equivalent to the state-based supervisor synthesis problem. This is formalized in the following theorem.

Theorem V.2. *Let $(M, \mathcal{F}_P^S, \mathcal{F}_S^R)$ be a Streett/Rabin supervisor synthesis automaton and $G(M)$ its associated game graph. Then there exists a state-based supervisor \tilde{f} that is a solution to the supervisor synthesis problem over $(M, \mathcal{F}_P^S, \mathcal{F}_S^R)$ iff*

there exists a player 0 strategy h winning the obliging game $(G(M), \mathcal{F}_{P \rightarrow S}^R, \mathcal{F}_P^S)$.

In order to prove Thm. V.2 we first formalize a mapping from paths over M to plays over G and back. This will allow us to define corresponding state-based supervisors and gracious strategies and formalize their associated properties in terms of (2) and (8).

Paths vs. Plays. To formally connect paths in M to plays over G , we define the set-valued map $\text{Plays} : x_0 X^* \rightarrow 2^{q_0(Q^1 Q^0)^*}$ iteratively as follows: $\text{Plays}(x_0) := \{x_0\}$ and $\text{Plays}(\nu x) := \{\mu \tilde{x} x \mid \mu \in \text{Plays}(\nu), \tilde{x} \in \{\text{Last}(\nu)\} \times \Gamma\}$. By slightly abusing notation, we extend the map Plays to infinite paths $\pi \in x_0 X^\omega$ as the limit of all mappings $\text{Plays}(p_n)$ where $(p_n) \in x_0 X^*$ is the unbounded monotone sequence of prefixes of π . Similarly, we define the inverse map $\text{Plays}^{-1} : q_0(Q^1 Q^0)^* \rightarrow x_0 X^*$ s.t. $\text{Plays}^{-1}(\mu) = \nu$ where ν is the single element of the set $\{\nu \in x_0 X^* \mid \mu \in \text{Plays}(\nu)\}$. Again we extend Plays^{-1} to infinite strings in the obvious way.

The construction of $G(M)$ from M in Def. IV.1 allows us to show that the map Plays indeed captures all the information required to map finite, infinite, and winning paths over M to the corresponding finite, infinite and winning plays over $G(M)$ and vice versa (see Lem. A.3 in App. C). That is, we have

$$\text{Plays}(\mathcal{P}(M)) = \mathcal{P}(G), \quad (9a)$$

$$\text{Plays}(\mathcal{P}(M)) = \mathcal{P}(G), \text{ and} \quad (9b)$$

$$\text{Plays}(\mathcal{P}(M, \mathcal{F})) = \mathcal{P}(G, \mathcal{F}), \quad (9c)$$

where \mathcal{F} is a winning condition over M .

Supervisors vs. Strategies. Unfortunately, we cannot directly utilize the properties in (9) to relate state-based supervisors and gracious strategies. By definition, control strategies can base their decision on all information from the past observed state sequence. As one path over M corresponds to multiple plays over $G(M)$, every such play could in principle induce a different control decision. We call strategies that do not utilize this additional flexibility *non-ambiguous*.

Definition V.1. Let G be as in Def. IV.1. We call a player 0 strategy over G *non-ambiguous* if for any $\nu \in x_0 X^*$ and any $\mu, \mu' \in \text{Plays}(\pi)$, we have $\tilde{h}(\mu) = \tilde{h}(\mu')$.

A strategy over G can only choose one particular next state in a current one. As the initial state is unique, there must be a unique control pattern chosen in this state leading to a unique next state in G . Iteratively applying this argument shows that there is a unique play over G generated under any control strategy h . Therefore, we can always construct a non-ambiguous strategy \tilde{h} over G from a given control strategy h with the same set of generated plays. This is formalized in the following proposition, which is proven in App. C.

Proposition V.3. *Given the premises of Lem. V.1, let h be a strategy over G , then \tilde{h} s.t.*

$$\tilde{h}(x_0) := h(x_0) \quad \text{and} \quad \tilde{h}(\mu \tilde{x}_k x_{k+1}) := h(\mu \tilde{h}(\mu) x_{k+1}) \quad (10)$$

is a non-ambiguous player 0 strategy over G and it holds that $\mathcal{P}(G, h) = \mathcal{P}(G, \tilde{h})$.

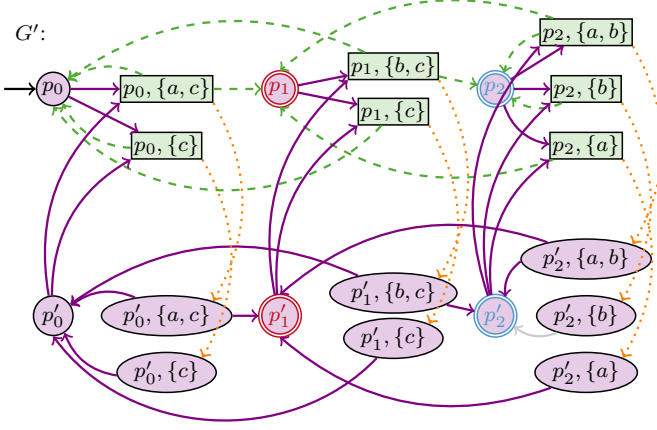


Fig. 3. Obliging game graph expansion of G in Fig. 2 as discussed in Sec. V-D (see [14] for a formalization). The plant can decide to chose the next event by herself (dashed green transitions) or to let the controller decide on her behalf (dotted orange transition followed by a solid violet one).

Prop. V.3 shows that restricting attention to non-ambiguous player 0 strategies over G is without loss of generality. Now it is easy to see that non-ambiguous strategies over $G(M)$ allow for a one-to-one correspondence with state-based supervisors over M , which finally leads to the desired correspondence between Problem 2 and Problem 3.

Proposition V.4. *Given the premises of Thm. V.2, let \check{h} be a non-ambiguous player 0 strategy over G and \check{f} a state-based supervisor for M s.t.*

$$\forall \mu \in q_0(Q^1 Q^0)^* . \check{h}(\mu) = (\text{Last}(\mu), \check{f}(\text{Plays}^{-1}(\mu))). \quad (11)$$

Then (2) holds for \check{f} iff (8) holds for \check{h} .

With this, we see that Thm. V.2 is an immediate corollary of Prop. V.3 and Prop. V.4.

D. Example

The technical reduction from obliging games to games with ω -regular winning conditions (see Thm. V.1) can be found in [14]. We give an intuitive explanation of this construction by applying it to our example and thereby constructing a winning strategy for the obliging game $(G(M), \mathcal{F}_{P \rightarrow S}^R, \mathcal{F}_P^S)$ over the game graph $G(M)$ depicted in Fig. 2.

As the first step of this construction, we double the state space of G resulting in an upper and a lower part (see Fig. 3). The upper part is a copy of the old state space while in the lower part all states become control player states (indicated by their violet ellipse shape). Now we run the following Gedankenexperiment: in every (rectangular green) state, the plant can chose between deciding on the next executed event by herself or allowing the controller to make this choice for her. In the first case the play stays within the upper part (using a dashed green transition), while in the second case the play moves to the lower part (using a dotted orange transition) and the controller decides the next move on behalf of the plant (by taking an available solid violet transition). In each case, the play moves to a control player's state (p_i (top) or p'_i (bottom), with $i \in \{0, 1, 2\}$). In both cases, the controller chooses a

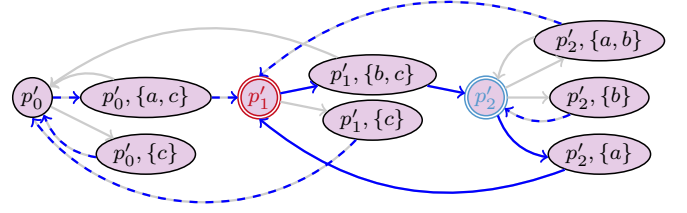


Fig. 4. Witness of a path from every reachable state of $G(M)$ (dashed) to a loop (solid) satisfying plant and specification makings always again. This defines a plant and control player strategy denoted by g^\downarrow and f^\downarrow , respectively.

control pattern γ and by this always moves to the rectangular green state (p_i, γ) in the upper part. Here, it is again the choice of the plant to either stay in the original (top) game or to move to the bottom copy.

With this modified game in mind, we can interpret the two copies of the game graph as follows. In the top one, the controller is only concerned with fulfilling the specification, i.e., solving a standard two-player game with the winning condition $\mathcal{F}_{P \rightarrow S}^R$ in (7).

The bottom copy of the game makes sure that the resulting strategy is non-conflicting. Within the outlined Gedankenexperiment, this is ensured by the fact that at any point in time, the plant can decide to hand over all future choices of the next events to the controller and the controller must be able to *demonstrate* that the liveness condition of the plant (i.e., \mathcal{F}_P^S) remains satisfiable along with satisfying $\mathcal{F}_{P \rightarrow S}^R$. Hence, from every reachable state in the top game, the controller must be able to give *one explicit trace* which visits both p'_1 and p'_2 always eventually again. This prevents the controller from moving to a state in the top game where the plant's assumptions are persistently violated. It should be noted that the synthesis problem over the lower game graph is actually much simpler, as it only involves one player (namely the controller) and thereby reduces to a simple path search.

A gracious strategy in the original obliging game is extracted from this Gedankenexperiment as follows. First, we consider the upper and the lower game in Fig. 3 separately. For the upper game, we know that a supervisor disabling events a and b in every state is winning w.r.t. $\mathcal{F}_{P \rightarrow S}^R$ (see Example IV.1). Call this strategy f^\uparrow . This strategy forces the plant to always remain in p_0 and wins in the upper game by vacuously satisfying the implication. For the lower part of the game, consider the blue transitions in Fig. 4, which indicate a particular infinite trace from every state which always eventually visits both p_1 and p_2 , and therefore fulfills both $\mathcal{S} = \mathcal{F}_{P \rightarrow S}^R$ and $\mathcal{W} = \mathcal{F}_P^S$. This path immediately defines a plant and a control player strategy which we denote g^\downarrow and f^\downarrow , respectively.

Given f^\uparrow , g^\downarrow , and f^\downarrow , we can combine them into a solution to the original synthesis problem over $G(M)$ (and therefore M) in Fig. 2, by adding one extra bit of memory to the controller. Intuitively, the controller tracks whether the system executes a move contained in g^\downarrow . If so, the controller executes the unique pattern chosen by f^\downarrow in the next state. Otherwise, it operates according to f^\uparrow . For the particular choices of strategies in this example we see that the only allowed event c in (p_0, γ) is part of g^\downarrow and therefore triggers f^\downarrow . Hence, the

actual closed loop allows the plant to move to p_1 next. If it does so, f^\downarrow remains active as this move is again contained in g^\downarrow (see Fig. 4). If the plant decides to stay in p_0 , f^\uparrow becomes active again. Intuitively, this way the controller tracks whether the plant is trying to make progress towards fulfilling her liveness condition. If so, he is cooperating with her to achieve this goal.

E. Algorithm

The reduction outlined in the previous section via Thm. III.1 and Thm. V.2 enables us to solve a given supervisory synthesis problem (Problem 1) over a plant model (L_P, \mathcal{L}_P) w.r.t. a specification \mathcal{L}_S and a set of uncontrollable events $\Sigma_{uc} \subseteq \Sigma$ through the following steps:

- 1) Construct a Street/Rabin synthesis automaton $(M, \mathcal{F}_P^S, \mathcal{F}_S^R)$ as in Def. III.1.
- 2) Extend M into a game graph $G(M)$ as in Def. IV.1.
- 3) Solve the obliging game $(G(M), \mathcal{F}_{P \rightarrow S}^R, \mathcal{F}_P^S)$ via its reduction to standard ω -regular games (see Thm. V.1).
- 4) If the obliging game has no solution, also Problem 1 has no solution (see Thm. III.1 and Thm. V.2).
- 5) If the obliging game allows for a control strategy h , compute its induced non-ambiguous strategy \tilde{h} as in (10).
- 6) Reduce \tilde{h} to a state-based supervisor via (12), which in turn defines the event-based supervisor f via (3).
- 7) Then f solves Problem 1 (see Thm. III.1 and Thm. V.2).

The complexity of this algorithm can be derived from Thm. V.1 in the following way. Given a synthesis automaton M with n states we get a game graph $G(M)$ with $n2^{|\Sigma_c|}$ states. Further, given the Streett and Rabin conditions \mathcal{F}_P^S and \mathcal{F}_S^R with l and k pairs, we get an obliging game having a strong Rabin condition with $l+k$ pairs and a weak Streett condition with l pairs. Finally, a parity game with \tilde{n} states and \tilde{k} parities can be solved in $O(\tilde{n}^{\tilde{k}})$ time. The resulting complexity of our algorithm is summarized in the following corollary.

Corollary 1. *The state-based supervisor synthesis problem over a synthesis automaton M with n states, equipped with the Streett and Rabin conditions \mathcal{F}_P^S and \mathcal{F}_S^R with l and k pairs, respectively, can be solved in time $O((n2^{|\Sigma_c|}(l+k)^2(l+k)!2^{O(l)})^{2(l+k)+2})$. If there is a supervisor, then there is a supervisor using $2(l+k) \cdot 2^{O(l)}$ memory.*

It should further be noted that checking if there is a state-based supervisor from a state is NP-complete [9]; this already holds for a trivial liveness assumption for the plant (i.e., $\mathcal{L}_P = \Sigma^\omega$) as solving Rabin games is NP-complete [26]. While our algorithm is sound and complete, it is possible that there is a more direct symbolic algorithm on the state space of the two-person game that yields a more efficient implementation. Such an algorithm is given in [24] for the special case where \mathcal{F}_P and \mathcal{F}_S are each a generalized Büchi winning condition. We postpone the generalization of this algorithm to future work.

REFERENCES

[1] P. J. Ramadge and W. M. Wonham, “Supervisory control of a class of discrete event processes,” *SIAM J. Control and Optimization*, vol. 25, pp. 206–230, 1987.

[2] C. G. Cassandras and S. LaFortune, *Introduction to Discrete Event Systems*, 2nd ed. Springer, 2008.

[3] W. M. Wonham and K. Cai, *Supervisory control of discrete-event systems*, ser. Communications and Control Engineering. Springer, 2019.

[4] W. Wonham, K. Cai, and K. Rudie, “Supervisory control of discrete-event systems: A brief history,” *Annual Reviews in Control*, 2018.

[5] S. LaFortune, “Discrete event systems: Modeling, observation, and control,” *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 2, pp. 141–159, 2019.

[6] J. G. Thistle and W. M. Wonham, “Control of ω -automata, church’s problem, and the emptiness problem for tree ω -automata,” in *International Workshop on Computer Science Logic*. Springer, 1991, pp. 367–381.

[7] —, “Supervision of infinite behavior of discrete-event systems,” *SIAM Journal on Control and Optimization*, vol. 32, no. 4, pp. 1098–1113, 1994.

[8] —, “Control of infinite behavior of finite automata,” *SIAM Journal on Control and Optimization*, vol. 32, no. 4, pp. 1075–1097, 1994.

[9] J. G. Thistle, “On control of systems modelled as deterministic rabin automata,” *Discrete Event Dynamic Systems*, vol. 5, no. 4, pp. 357–381, 1995.

[10] A. Church, “Applications of recursive arithmetic to the problem of circuit synthesis,” *Summaries of the Summer Institute of Symbolic Logic, Volume I*, pp. 3–50, 1957.

[11] R. Ehlers, S. LaFortune, S. Tripakis, and M. Y. Vardi, “Supervisory control and reactive synthesis: a comparative introduction,” *Discrete Event Dynamic Systems*, vol. 27, no. 2, pp. 209–260, 2017.

[12] A.-K. Schmuck, T. Moor, and R. Majumdar, “On the relation between reactive synthesis and supervisory control of non-terminating processes,” *Discrete Event Dynamic Systems*, vol. 30, pp. 81–124, 2020.

[13] O. Kupferman and M. Y. Vardi, “Safraless decision procedures,” in *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS’05)*. IEEE, 2005, pp. 531–540.

[14] K. Chatterjee, F. Horn, and C. Löding, “Obliging games,” in *International Conference on Concurrency Theory*. Springer, 2010, pp. 284–296.

[15] A. Schmuck, T. Moor, and K. W. Schmidt, “A reactive synthesis approach to supervisory control of terminating processes,” in *21st IFAC World Congress, Berlin, Germany, July 12-17, 2020*, 2020, p. (to appear).

[16] Z. Ramezani, J. Krook, Z. Fei, M. Fabian, and K. Akesson, “Comparative case studies of reactive synthesis and supervisory control,” in *2019 18th European Control Conference (ECC)*. IEEE, 2019, pp. 1752–1759.

[17] A. Sakakibara and T. Ushio, “Hierarchical control of concurrent discrete event systems with linear temporal logic specifications,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E101.A, no. 2, pp. 313–321, 2018.

[18] S. Jiang and R. Kumar, “Supervisory control of discrete event systems with ctl* temporal logic specifications,” *SIAM Journal on Control and Optimization*, vol. 44, no. 6, pp. 2079–2103, 2006.

[19] G. Aucher, “Supervisory control theory in epistemic temporal logic,” in *AAMAS ’14*, 2014, pp. 333–340.

[20] A. C. van Hulst, M. A. Reniers, and W. J. Fokkink, “Maximally permissive controlled system synthesis for non-determinism and modal logic,” *Discrete Event Dynamic Systems*, vol. 27, no. 1, pp. 109–142, Mar 2017.

[21] J.-M. Yang, T. Moor, and J. Raisch, “Refinements of behavioural abstractions for the supervisory control of hybrid systems,” *Discrete Event Dynamic Systems*, pp. 1–28, 2020.

[22] C. Baier and T. Moor, “A hierarchical control architecture for sequential behaviours,” *IFAC Proceedings Volumes*, vol. 45, no. 29, pp. 259–264, 2012.

[23] T. Moor, “Supervisory control on non-terminating processes: An interpretation of liveness properties,” *Lehrstuhl für Regelungstechnik, Friedrich-Alexander Universität Erlangen-Nürnberg*, Tech. Rep., 2017.

[24] R. Majumdar, N. Piterman, and A.-K. Schmuck, “Environmentally-friendly gr (1) synthesis,” in *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer, 2019, pp. 229–246.

[25] A. Pnueli and R. Rosner, “On the synthesis of a reactive module,” in *Proceedings of the 16th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, 1989, pp. 179–190.

[26] E. A. Emerson and C. S. Jutla, “The complexity of tree automata and logics of programs,” in *FoCS*, vol. 88. Citeseer, 1988, pp. 328–337.

[27] E. Emerson and C. Jutla, “Tree automata, mu-calculus and determinacy,” in *FOCS’91*, Oct 1991, pp. 368–377.

[28] W. Thomas, “On the synthesis of strategies in infinite games,” in *STACS’95 Munich, Germany*, 1995, pp. 1–13.

APPENDIX

A. Proof of Thm. III.1

We prove both directions of Thm. III.1 separately by the following two lemmas.

Lemma A.1. *Given the premises of Thm. III.1, let $f : \Sigma^* \rightarrow \Gamma$ be a solution to Problem 1 and define $\check{f} : P(M) \rightarrow \Gamma$ s.t. $\check{f}(\rho) = f(\text{Paths}_M^{-1}(\rho))$. Then \check{f} is a solution to Problem 2.*

Proof. Fix $f : \Sigma^* \rightarrow \Gamma$ s.t. (1a) and (1b) holds, and let \check{f} be as in Lem. A.1. We show that (2a) and (2b) hold for \check{f} .

► Show (2a): ▸ Show $\mathcal{P}(M, \check{f}) \cap \mathcal{P}(M, \mathcal{F}_P) \neq \emptyset$: As $\mathcal{L}_f \cap \mathcal{L}_P \neq \emptyset$ (from (1a)), there exists a string $s \in \mathcal{L}_P$ which is infinite and consistent with f , i.e., for all $\sigma \in \Sigma$ and $t\sigma \in \text{pfx}(s)$ holds that $\sigma \in f(t)$. As M is deterministic, we have $|\text{Paths}_M(s)| = 1$ and we can define $\pi := \text{Paths}_M(s)$. With $\mathcal{L}_P := \mathcal{L}(M, \mathcal{F}_P)$ we have $\pi \in \mathcal{P}(M, \mathcal{F}_P)$. As M is deterministic, we have $\text{Paths}_M(t\sigma) \in \text{pfx}(\pi) \in P(M)$ for all $t\sigma \in \text{pfx}(s)$. This implies $\pi \in \mathcal{P}(M, \check{f})$ by construction of \check{f} , i.e., $\pi \in \mathcal{P}(M, \check{f}) \cap \mathcal{P}(M, \mathcal{F}_P)$ which proves the statement.

▸ Show $\pi \in \mathcal{P}(M, \mathcal{F}_S)$: Recall from the proof of the previous claim, that $s = \text{Paths}_M^{-1}(\pi) \in \mathcal{L}_f \cap \mathcal{L}_P$. As (1a) holds, this implies $s \in \mathcal{L}_S$. From $\mathcal{L}_S := \mathcal{L}(M, \mathcal{F}_S)$ it follows that $\pi \in \mathcal{P}(M, \mathcal{F}_S)$.

► Show (2b): Pick $\nu \in P(M, \check{f})$ and observe that this implies $\nu \in P(M)$. As $L_P := \mathcal{L}(M)$ this implies that $t = \text{Paths}_M^{-1}(\nu) \in L_P$. Further, it follows from the properties of M that $t \in L_f$. As (1b) holds, this implies $t \in \text{pfx}(\mathcal{L}_f \cap \mathcal{L}_P)$ and thereby $\nu \in \text{pfx}(\mathcal{P}(M, \check{f}) \cap \mathcal{P}(M, \mathcal{F}_P))$. ■

Lemma A.2. *Given the premises of Thm. III.1, let $\check{f} : P(M) \rightarrow \Gamma$ be a solution to Problem 2 and define $f : \Sigma^* \rightarrow \Gamma$ s.t. $f(s) = \check{f}(\text{Paths}_M(s))$ if $s \in L(M)$. Then f is a solution to Problem 1.*

Proof. Fix \check{f} s.t. (2) holds, and let f be as in Lem. A.2. We show that (1a) and (1b) hold for f .

► Show (1a): ▸ Show $\mathcal{L}_f \cap \mathcal{L}_P \neq \emptyset$: Recall that $\mathcal{P}(M, \check{f}) \cap \mathcal{P}(M, \mathcal{F}_P) \neq \emptyset$ from (2a). Hence, there exists a path $\pi \in \mathcal{P}(M, \mathcal{F}_P)$ which is consistent with \check{f} , that is, for all $x, x' \in X$ and $\nu xx' \in \text{pfx}(\pi)$ holds that there exists an $\sigma \in \check{f}(\nu x)$ s.t. $x' = \delta(x, \sigma)$. As M has unique transition labels (Def. III.1 (b)), we have $|\text{Paths}_M^{-1}(\pi)| = 1$ and we can define $s := \text{Paths}_M^{-1}(\pi)$. With $\mathcal{L}_P := \mathcal{L}(M, \mathcal{F}_P)$ we further have $s \in \mathcal{L}_P$. As M has unique transition labels, we further have $\text{Paths}_M^{-1}(\nu x) \in \text{pfx}(s) \in L_P = L(M)$ for all $\nu x \in \text{pfx}(\pi)$. This implies $s \in \mathcal{L}_f$ by construction of f , which proves the statement.

▸ Show $s \in \mathcal{L}_S$: Recall that $\pi = \text{Paths}_M(s)$ is unique and $\pi \in \mathcal{P}(M, \check{f}) \cap \mathcal{P}(M, \mathcal{F}_P)$. As (2a) holds, this implies $\pi \in \mathcal{P}(M, \mathcal{F}_S)$. From $\mathcal{L}_S := \mathcal{L}(M, \mathcal{F}_S)$ and the construction of f it therefore follows that $s \in \mathcal{L}_S$.

► Show (1b): Pick $t \in L_f \cap L_P$ and recall that $L_P = L(M)$. With this, we have $t \in L(M)$ and therefore $\nu := \text{Paths}_M(t) \in P(M, \check{f})$ by construction of f . As (2a) holds, this implies $\nu \in \text{pfx}(\mathcal{P}(M, \check{f}) \cap \mathcal{P}(M, \mathcal{F}_P))$ and thereby $t \in \text{pfx}(\mathcal{L}_f \cap \mathcal{L}_P)$. ■

B. Proof of Thm. V.1

The first claim of Thm. V.1 immediately follows from [14, Thm.3].

For the complexity of the reduction in the special case of a strong Rabin and a weak Street condition, the claimed complexity of the reduction occurs as follows. Suppose G has n states and the Streett and Rabin conditions \mathcal{F}^S and \mathcal{F}^R have l and k pairs, respectively. From a Streett condition with l pairs, one can construct a (not necessarily deterministic) Büchi automaton with $2^{O(l)}$ states that accepts the same language. Moreover, by taking a product with a monitor with $k^2 \cdot k!$ states, we can convert the Rabin winning condition to a parity condition [27] with $2k$ parities.

Now, the reduction in [14, Lem.2, Thm.4] reduces a game with \tilde{n} states, a strong winning condition given by a parity condition with $2k$ parities and a weak winning condition accepted by a (not necessarily deterministic) Büchi automaton with q states into a game with $O(\tilde{n}q)$ states, $2k + 2$ parities, and memory $2qk$.

Applying this reduction to our setting and composing the above reductions, we get a parity game with $n \cdot k^2 \cdot k! \cdot 2^{O(l)}$ states, $2k + 2$ parity conditions, and memory $2k \cdot 2^{O(l)}$.

C. Proof of Thm. V.2

We have the following obvious properties of the map Plays and its inverse Plays^{-1} that we will utilize to prove Thm. V.2.

Let $A, A', B \subseteq x_0 X^*$ s.t. $A \subseteq A'$ then
 [Prop.a] $\text{Plays}(A) \subseteq \text{Plays}(A')$,
 [Prop.b] $\text{pfx}(\text{Plays}(A)) = \text{Plays}(\text{pfx}(A))$, and
 [Prop.c] $\text{Plays}(A \cap B) = \text{Plays}(A) \cap \text{Plays}(B)$.
 Conversely, let $A, A', B \subseteq q_0(Q^1 Q^0)^*$ s.t. $A \subseteq A'$ then
 [Prop.d] $\text{Plays}^{-1}(A) \subseteq \text{Plays}^{-1}(A')$,
 [Prop.e] $\text{pfx}(\text{Plays}^{-1}(A)) = \text{Plays}^{-1}(\text{pfx}(A))$, and
 [Prop.f] $\text{Plays}^{-1}(A \cap B) = \text{Plays}^{-1}(A) \cap \text{Plays}^{-1}(B)$.

With this, we can formalize the correspondences between paths over M and plays over its induced game graph $G(M)$.

Lemma A.3. *Let M be an automaton as in Def. III.1 and let $G(M)$ its associated game graph as in Def. IV.1. Then*

- (i) $\text{Plays}(\text{pfx}(\mathcal{P}(M))) \subseteq \text{pfx}(\mathcal{P}(G))$ and in particular $\text{Plays}(\mathcal{P}(M)) \subseteq \mathcal{P}(G)$, and
- (ii) $\text{Plays}^{-1}(\text{pfx}(\mathcal{P}(G))) \subseteq \text{pfx}(\mathcal{P}(M))$ and in particular $\text{Plays}^{-1}(\mathcal{P}(G)) \subseteq \mathcal{P}(M)$.

Further, let \mathcal{F} be a winning condition over M . Then

- (iii) \mathcal{F} is a winning condition over G , and
- (iv) $\text{Plays}(\mathcal{P}(M, \mathcal{F})) = \mathcal{P}(G, \mathcal{F})$.

Proof. We show all claims separately.

► (i) For the first claim, let $\nu = x_0 x_1 \dots x_k \in \text{pfx}(\mathcal{L}(M))$. Then it immediately follows from the definitions that $\text{Plays}(\nu)$ is exactly the set containing all plays $x_0(x_0, \gamma_0)x_1(x_1, \gamma_1) \dots (x_k, \gamma_{k-1})x_k$ s.t. $\gamma_i \in \Gamma$ for all $i \in [0; k]$. Then it follows from Def. IV.1 that all $\mu \in \text{Plays}(\nu)$ are indeed a play over G starting in q_0 , and, hence $\text{Plays}(\text{pfx}(\mathcal{P}(M))) \subseteq \text{pfx}(\mathcal{P}(G))$. The second claim immediately follows from the closure over the first.

► (ii) For the first claim, let $\mu = x_0(x_0, \gamma_0)x_1(x_1, \gamma_1) \dots (x_k, \gamma_{k-1})x_k \in \text{pfx}(\mathcal{P}(G))$ and

observe that $\text{Plays}^{-1}(\mu) = x_0x_1 \dots x_k$. Now it follows from the last condition in Def. IV.1 that for each $i \in [1; k]$ there exists a σ_i s.t. $x_i = \delta(x_{i-1}, \sigma_i)$. Therefore ν is a path in M and the claim is proven. The second claim immediately follows from the closure over the first.

► (iii) This claim trivially follows from the fact that $Q = Q^0 \cup Q^1$ with $Q^0 = X$. As $\mathcal{F} = \{\langle G_1, R_1 \rangle, \dots, \langle G_m, R_m \rangle\}$ s.t. $G_i, R_i \subseteq X$ for all $i \in [1; m]$, we immediately also have $G_i, R_i \subseteq Q$ for all $i \in [1; m]$, what proves the statement.

► (iv) For the inclusion “ \subseteq ”, pick any path $\pi \in \mathcal{P}(M, \mathcal{F})$. Then we know that the set $\text{Inf}(\pi) \subseteq X$ fulfills the conditions for acceptance w.r.t. the acceptance condition \mathcal{F} over M . Now take any $\rho \in \text{Plays}(\pi) \subseteq \mathcal{P}(G)$ and observe that deciding winning of ρ w.r.t. $\mathcal{F} \subseteq Q^0$ only depends on the set $\text{Inf}(\rho)|_{Q^0} \subseteq Q^0$. Then the claim follows from the observation that the definition of Plays implies $\text{Inf}(\rho)|_{Q^0} = \text{Inf}(\pi)$. The reverse inclusion proceeds identically and is omitted. ■

This now enables us to prove Prop. V.3 on page 6.

Proof of Prop. V.3. We show the claim by induction.

▷ For the base-case, observe that there is a unique choice of h at the initial state $q_0 = x_0$ and that $\text{Plays}(x_0) = \{x_0\}$. We therefore obviously have that for all $\mu, \mu' \in \text{Plays}(x_0)$ we have $\mu = \mu' = x_0$ and hence $\check{h}(\mu) = \check{h}(\mu') = h(x_0)$. This further implies, $\mathcal{P}(G, h)|_{[0,0]} = \mathcal{P}(G, \check{h})|_{[0,0]}$.

▷ For the induction step, fix $\nu \in x_0X^*$ with $|\nu| = k > 1$ and assume that for all $\mu, \mu' \in \text{Plays}(\nu)$ we have $h(\mu) = \check{h}(\mu')$. Now choose any $x \in X$ and observe that $\text{Plays}(\nu x) = \{\mu \tilde{x} \mid \mu \in \text{Plays}(\nu), \tilde{x} \in \{\text{Last}(\nu)\} \times \Gamma\}$. Now pick any two $\mu \tilde{x}, \mu' \tilde{x}' \in \text{Plays}(\nu x)$ and observe that from the definition of \check{h} follows that $\check{h}(\mu \tilde{x}) = h(\mu \check{h}(\mu)x)$ and $\check{h}(\mu' \tilde{x}') = h(\mu' \check{h}(\mu')x)$. As $\mu, \mu' \in \text{Plays}(\nu)$ it follows from the induction hypothesis that $\check{h}(\mu) = \check{h}(\mu')$ and therefore $\check{h}(\mu \tilde{x}) = \check{h}(\mu' \tilde{x}')$. This proves that \check{h} is non-ambiguous.

▷ Now assume $\Lambda := \mathcal{P}(G, h)|_{[0,k]} = \mathcal{P}(G, \check{h})|_{[0,k]}$ and $\check{h}(\mu) = h(\mu)$ for all $\mu \in \Lambda$. Then it follows from Def. IV.1 that $\mathcal{P}(G, h')|_{[0,k+2]}$ contains all strings $\mu(\text{Last}(\mu), \gamma)x'$ s.t. $\mu \in \Lambda$, $(\text{Last}(\mu), \gamma) = h'(\mu)$ and $x' = \delta(x_0, \sigma)$ for some $\sigma \in \gamma$. With this it immediately follows from the induction hypothesis that $\mathcal{P}(G, h)|_{[0,k+2]} = \mathcal{P}(G, \check{h})|_{[0,k+2]}$. As both $\mathcal{P}(G, h)$ and $\mathcal{P}(G, \check{h})$ are closed languages, this proves the claim. ■

Prop. V.3 shows that restricting attention to non-ambiguous player 0 strategies over G is without loss of generality. In fact, this introduces an immediate correspondence between non-ambiguous strategies over $G(M)$ and state-based supervisors over M , as formalized in the following lemma.

Lemma A.4. *Given the premises of Lem. A.3 the following holds.*

(i) *Let \check{f} be a state-based supervisor for M and \check{h} s.t.*

$$\check{h}(\mu) = (\text{Last}(\mu), \check{f}(\text{Plays}^{-1}(\mu))). \quad (12)$$

Then \check{h} is a non-ambiguous player-0 strategy over G and it holds that $\mathcal{P}(G, \check{h}) = \text{Plays}(\mathcal{P}(M, \check{f}))$.

(ii) *Let h be a player 0 strategy over G , \check{h} its non-ambiguous reduction as in (10), and \check{f} s.t.*

$$\check{f}(\nu) = \gamma \text{ with } \gamma \in \{\exists \mu \in \text{Plays}(\nu) \cdot \check{h}(\mu) = (\cdot, \gamma)\}. \quad (13)$$

Then \check{f} is a state-based supervisor for M and $\mathcal{P}(G, h) = \text{Plays}(\mathcal{P}(M, \check{f}))$.

Proof. We prove both statements separately.

► (i) Non-ambiguity of \check{h} follows by construction, as for any $\nu \in x_0X^*$ and $\mu, \mu' \in \text{Plays}(\nu)$ we have $\text{Last}(\mu) = \text{Last}(\mu') = \text{Last}(\nu)$ and therefore $\check{h}(\mu) = (\text{Last}(\mu), \check{f}(\nu)) = (\text{Last}(\mu'), \check{f}(\nu)) = \check{h}(\mu')$. We now prove $\mathcal{P}(G, \check{h}) = \text{Plays}(\mathcal{P}(M, \check{f}))$ by induction.

▷ For the base case observe that $x_0 = q_0$ and $\text{Plays}^{-1}(q_0) = x_0$. We therefore have $\mathcal{P}(G, \check{h})|_{[0,0]} = \text{Plays}(\mathcal{P}(M, \check{f}))|_{[0,0]}$ and $\check{h}(q_0) = \check{f}(\text{Plays}^{-1}(q_0))$.

▷ For the induction step, assume $\Lambda = \mathcal{P}(G, \check{h})|_{[0,k]} = \text{Plays}(\mathcal{P}(M, \check{f}))|_{[0,k]}$ and $\check{h}(\mu) = \check{f}(\text{Plays}^{-1}(\mu))$ for all $\mu \in \Lambda$. Then it follows from Def. IV.1 that $\mathcal{P}(G, \check{h})|_{[0,k+2]}$ contains all strings $\mu(\text{Last}(\mu), \gamma)x'$ s.t. $\mu \in \Lambda$, $(\text{Last}(\mu), \gamma) = \check{h}(\mu)$ and $x' = \delta(x_0, \sigma)$ for some $\sigma \in \gamma$. With this it immediately follows from the induction hypothesis and the definition of Plays that $\mathcal{P}(G, h)|_{[0,k+2]} = \text{Plays}(\mathcal{P}(M, \check{f}))|_{[0,k+2]}$. As both $\mathcal{P}(G, h)$ and $\mathcal{P}(M, \check{f})$ are closed languages, this proves the claim.

► First, observe that non-ambiguity of \check{h} implies uniqueness of γ in (13) defined for any x_0X^* , which makes it a state-based supervisor for M . Further, observe, that for \check{h} from (ii) and \check{f} in (13) again (12) holds. With this, we obtain $\mathcal{P}(G, \check{h}) = \text{Plays}(\mathcal{P}(M, \check{f}))$ from (i). Finally, $\mathcal{P}(G, h) = \mathcal{P}(G, \check{h})$ follows from Prop. V.3. ■

With this correspondence in place, we can finally prove Prop. V.4 on page 7.

Proof of Prop. V.4. ► (i) “ \Rightarrow ” Recall that $\mathcal{P}(G, \check{h}) = \text{Plays}(\mathcal{P}(M, \check{f}))$ from Lem. A.4 (i), $\text{Plays}(\mathcal{P}(M, \check{f})) \subseteq \text{Plays}(\mathcal{P}(M, \mathcal{S}))$ from [Prop.a] and the equivalence of (2a) and (6), and $\text{Plays}(\mathcal{P}(M, \mathcal{S})) = \mathcal{P}(M, \mathcal{S})$ from Lem. A.3. Combining all statements yields $\mathcal{P}(G, \check{h}) \subseteq \mathcal{P}(G, \mathcal{S})$.

► (i) “ \Leftarrow ” The proof is almost identical to the reverse direction. We have $\mathcal{P}(M, \check{f}) = \text{Plays}^{-1}(\mathcal{P}(G, \check{h}))$ from Lem. A.4 (i), $\text{Plays}^{-1}(\mathcal{P}(G, \check{h})) \subseteq \text{Plays}^{-1}(\mathcal{P}(G, \mathcal{S}))$ from [Prop.d] and (??), and $\text{Plays}(\mathcal{P}(M, \mathcal{S})) = \mathcal{P}(M, \mathcal{S})$ from Lem. A.3. Combining all statements yields $\mathcal{P}(M, \check{f}) \subseteq \mathcal{P}(M, \mathcal{S})$ which is equivalent to (2a) and therefore proves the statement.

► (ii) “ \Rightarrow ” We have $\text{pfx}(\mathcal{P}(G, \check{h})) = \text{pfx}(\text{Plays}(\mathcal{P}(M, \check{f})))$ from Lem. A.4 (i), $\text{pfx}(\text{Plays}(\mathcal{P}(M, \check{f}))) = \text{Plays}(\text{pfx}(\mathcal{P}(M, \check{f})))$ from [Prop.a], $\text{Plays}(\text{pfx}(\mathcal{P}(M, \check{f}))) \subseteq \text{Plays}(\text{pfx}(\mathcal{P}(M, \check{f}) \cap \mathcal{P}(M, \mathcal{W})))$ from (2b), $\text{Plays}(\text{pfx}(\mathcal{P}(M, \check{f}) \cap \mathcal{P}(M, \mathcal{W}))) = \text{pfx}(\text{Plays}(\mathcal{P}(M, \check{f}) \cap \text{Plays}(\mathcal{P}(M, \mathcal{W}))))$ from [Prop.c] and $\text{Plays}(\mathcal{P}(M, \check{f})) = \mathcal{P}(G, \check{h})$ from Lem. A.4 and $\text{Plays}(\mathcal{P}(M, \mathcal{W})) = \mathcal{P}(G, \mathcal{W})$ from Lem. A.3. Combining all statements yields $\text{pfx}(\mathcal{P}(G, \check{h})) \subseteq \text{pfx}(\mathcal{P}(G, \check{h}) \cap \mathcal{P}(G, \mathcal{W}))$.

► (ii) “ \Leftarrow ” This proof is almost identical to the inverse direction and therefore omitted. ■