

# Adapting Behaviors via Reactive Synthesis

Gal Amram<sup>1</sup>, Suguman Bansal<sup>2</sup>, Dror Fried<sup>3</sup>, Lucas M. Tabajara<sup>4</sup>, Moshe Y. Vardi<sup>4</sup>, and Gera Weiss<sup>5</sup>

<sup>1</sup> Tel-Aviv University, Israel [galam1483@gmail.com](mailto:galam1483@gmail.com)

<sup>2</sup> University of Pennsylvania, USA [suguman@seas.upenn.edu](mailto:suguman@seas.upenn.edu)

<sup>3</sup> The Open University of Israel, Israel [dfried@openu.ac.il](mailto:dfried@openu.ac.il)

<sup>4</sup> Rice University, USA [{lucasmt, vardi}@rice.edu](mailto:{lucasmt, vardi}@rice.edu)

<sup>5</sup> Ben-Gurion University of the Negev, Israel [geraw@bgu.ac.il](mailto:geraw@bgu.ac.il)

**Abstract.** In the *Adapter Design Pattern*, a programmer implements a *Target* interface by constructing an *Adapter* that accesses an existing *Adaptee* code. In this work, we present a reactive synthesis interpretation to the adapter design pattern, wherein an algorithm takes an *Adaptee* and a *Target* transducers, and the aim is to synthesize an *Adapter* transducer that, when composed with the *Adaptee*, generates a behavior that is equivalent to the behavior of the *Target*. One use of such an algorithm is to synthesize controllers that achieve similar goals on different hardware platforms. While this problem can be solved with existing synthesis algorithms, current state-of-the-art tools fail to scale. To cope with the computational complexity of the problem, we introduce a special form of specification format, called *Separated GR(k)*, which can be solved with a scalable synthesis algorithm but still allows for a large set of realistic specifications. We solve the realizability and the synthesis problems for Separated GR(k), and show how to exploit the separated nature of our specification to construct better algorithms, in terms of time complexity, than known algorithms for GR(k) synthesis. We then describe a tool, called SGR(k), that we have implemented based on the above approach and show, by experimental evaluation, how our tool outperforms current state-of-the-art tools on various benchmarks and test-cases.

## 1 Introduction

Inspired by the well known adapter design pattern [23], we study the use of reactive synthesis for generating adapters that translate inputs meant for a target transducer to inputs of an adaptee transducer. Consider, as one motivating example, the practice of adding code to an operating system that mitigates the risk posed by newly discovered hardware vulnerabilities like Spectre and Melt-down [29, 34]. While the discovery of such vulnerabilities puts constraints on how the hardware can be used, the patch of the operating system (called adapter in this paper) takes upon itself to take care of running all applications without change [31]. It does so by allowing applications of the existing interface, while adapting their operation in way that ensures that the system is not exposed to the new threat.

Formally, we propose the following synthesis problem: given two finite-state transducers called *Target* and *Adaptee*, synthesize a finite-state transducer called *Adapter* such that

$$\text{Adaptee} \circ \text{Adapter} \approx \text{Target}.$$

The symbol  $\circ$  stands for standard transducer composition [36] and the symbol  $\approx$  stands for an equivalence relation, a generalization of sequential equality, which we explain below. In words, we want an *Adapter* that stands between an *Adaptee* and its inputs and guarantees, such that the composition  $\text{Adaptee} \circ \text{Adapter}$  is equivalent to *Target*. In the vulnerability patching example, *Adaptee* is a model of the constrained hardware and *Target* is a model of the hardware as used before the discovery of the vulnerability, without the new constraints. The *Adapter* that we generate models the patch that mediates between the vulnerable hardware and applications that are not aware of the vulnerability.

In our setting, an input to the synthesis algorithm is the equivalence relation along with the specification of the adaptee and of the target. While the problem of synthesizing an adapter such that  $\text{Adaptee} \circ \text{Adapter}$  is sequentially equal to *Target* may be useful in some cases [45], we study here a more general problem. This is called for by applications such as the vulnerability covering patches described above. Specifically, we allow our users to specify an equivalence relation between  $\text{Adaptee} \circ \text{Adapter}$  and *Target* that is not necessarily sequential equality. In this paper, we propose to use  $\omega$ -regular properties [3] for specifying this equivalence relation, as follows. We assume, without loss of generality, that the outputs of both the *Target* and the *Adaptee* are assignments to disjoint sets of atomic propositions. We then consider sequences of pairs of such assignments that correspond to zipped runs of  $\text{Adaptee} \circ \text{Adapter}$  and of *Target* over the same input. Having this set of sequences in mind, the user specifies a set of temporal properties using an  $\omega$ -regular formalism such as LTL or Büchi automata. The transducer  $\text{Adaptee} \circ \text{Adapter}$  is considered equivalent to *Target* if all the properties that the user specified are satisfied for each sequence in the set [24]. Note that the equivalence relation can be very different than sequential equality, it can, for example, say that  $\text{Adaptee} \circ \text{Adapter}$  must be, in a way, a “mirror image” of *Target*, as demonstrated by the cleaning robots example in Section 4.1, where *Target* is a robot that cleans some rooms and  $\text{Adaptee} \circ \text{Adapter}$  is a robot that clean all the rooms that *Target* did not clean.

The solution that we propose in this paper consists of two phases: we first transform the transducers to transition systems and arrive at a game structure that is more amenable for game-based techniques. Then we make use of the specific form of the resulting game and some simplifying assumptions about the form of the equivalence properties to solve the game efficiently. The game structures that we analyze consist of pairs of transition systems called *Input* and *Output*, accompanied by a set of  $\omega$ -regular properties that specify equivalence relation between the two, as described above. The game that we solve is, then, to find a controller that reads the assignments to the variables of the *Input* and produces a valid sequence of assignments to the variables of the *Output* such that all the properties are satisfied. The translation of the transducers to this

game structure is rather direct, as elaborated in Section 4. The *Input* transition system is generated from the *Target* transducer and the *Output* transition system is generated from the *Adaptee* transducer. This is because we want the *Adapter*, which we generate from the controller as described below, to consider the behavior of the *Target* and to translate it to a command that generates an equivalent behaviour of *Adaptee*. Once we find a controller that solves the game, we can transform it to an adapter we detail in Section 4.

The synthesis problem that we defined so far is as hard computationally as general LTL synthesis and is thus double exponential in the worst case [51]. To cope with this difficulty, we propose to use a well known fragment of LTL called  $\text{GR}(k)$ .  $\text{GR}(k)$  generalizes the  $\text{GR}(1)$  subset of LTL [11], a practical fragment of LTL for which a feasible reactive synthesis algorithm exists (see, e.g., [10, 32, 39, 46, 47, 53]). Furthermore,  $\text{GR}(k)$  formulas are known to be highly expressive, as they can encode most commonly appearing LTL industrial patterns [19, 40, 42] and DBA properties (see related works for details). In addition to using  $\text{GR}(k)$ , since the *Input* and *Output* in our model are separated transition systems, with separated sets of atomic propositions, we focus on properties that separate input and output variables. That is, our specification has the form  $\bigwedge_{i=1}^k (\phi_i \rightarrow \psi_i)$ , where the  $\phi_i$  and  $\psi_i$  are conjunctions of LTL  $\text{GF}$  (Globally in the Future) formulas over *Input* variables only and *Output* variables only respectively. We call this model *Separated GR(k)*. We show through several case-studies that this fragment of LTL suffices to specify a range of useful equivalence relations.

We study the problems of realizability and synthesis on Separated  $\text{GR}(k)$  game. For that, we first consider a sub-problem of solving a *weak Büchi* game. Then we identify and make use of a property of separated games that we call *delay property*: the system can delay its response to the environment indefinitely as long as it remains in the same connected component of the game graph. This allows us to decide the realizability of Separated  $\text{GR}(k)$  in  $O(|\varphi| + N)$  symbolic operations, and to synthesize a controller for a realizable specification in  $O(|\varphi|N)$  symbolic operations, where  $\varphi$  is the Separated  $\text{GR}(k)$  specification, and  $N$  is the size of the state-space. Thus, Separated  $\text{GR}(k)$  games are easier to solve than solving  $\text{GR}(k)$  games which require  $O(N^{k+1}k!)$  operations [49]. This demonstrates the efficiency of our framework, since  $|\varphi|$  tends to be smaller than  $N$  and in most practical cases,  $|\varphi| \in O(\log(N))$ .

The benefits of the complexity-theoretic improvement are reflected in empirical evaluations on our case studies of separated  $\text{GR}(k)$  formulas. We demonstrate that while separated  $\text{GR}(k)$  formulas are challenging for state-of-the-art synthesis tools, a symbolic BDD-based implementation of our algorithm solves them scalably and efficiently.

The rest of the paper is organized as follows: Section 2 introduces necessary preliminaries. Separated  $\text{GR}(k)$  games are introduced and formulated in Section 3. In Section 4 we describe how to use Separated  $\text{GR}(k)$  games synthesis to generate the adapter transducer, and introduce several use-cases. Next, we turn to solving separated  $\text{GR}(k)$  games. An overview of our solution approach and a necessary property for correctness of algorithm, called the delay property,

is given in Section 5. A complete symbolic algorithm is presented in Section 6. An empirical evaluation on case-studies is presented in Section 7. Finally, in Section 8 and Section 9 respectively, we give related work and conclude.

## 2 Preliminaries

**General Definitions.** Given a set of Boolean variables  $\mathcal{V}$ , a *state over  $\mathcal{V}$*  is an assignment  $s$  to the variables in  $\mathcal{V}$ . We describe  $s$  as the subset of  $\mathcal{V}$  that is assigned **True** in  $s$ . The set of *primed variables of  $\mathcal{V}$*  is  $\mathcal{V}' = \{v' \mid v \in \mathcal{V}\}$ . Then  $s' = \{v' \mid v \in s\}$  is the primed state  $s'$  over  $\mathcal{V}'$ . An *assertion over  $\mathcal{V}$*  is a Boolean formula over variables  $\mathcal{V}$ . A state  $s$  satisfies an assertion  $\rho$  over the same variables, denoted  $s \models \rho$ , if  $\rho$  evaluates to **True** by assigning *true* to the elements of  $s$ . We define the *projection* of a state  $s$  on a subset  $\mathcal{U} \subseteq \mathcal{V}$  as denoted by  $s|_{\mathcal{U}} = s \cap \mathcal{U}$ . We extend the notion of projection to a set of states  $S \subseteq 2^{\mathcal{V}}$  by defining  $S|_{\mathcal{U}} = \{s|_{\mathcal{U}} \mid s \in S\}$ .

Our specification is a special form of *Linear Temporal Logic (LTL)*. LTL [50] extends propositional logic with infinite-horizon temporal operators. The syntax of an LTL formula over a finite set of Boolean variables  $\mathcal{V}$  is defined as follows:  $\varphi ::= v \in \mathcal{V} \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathbf{X}\varphi \mid \varphi \mathbf{U}\varphi \mid \mathbf{F}\varphi \mid \mathbf{G}\varphi$ . Here **X** (Next), **U** (Until), **F** (Eventually), **G** (Always) are temporal operators. The semantics of LTL can be found in [6, Chapter 5].

We model the adapters as transducers. A *transducer* is a deterministic finite-state machine with no accepting states, but with additional output alphabet and an additional function from the set of states to the output alphabet. A formal definition of a transducer can be found in [21], but is not required for this paper.

The algorithms developed in this paper are symbolic, i.e. manipulate implicit representations of sets of states. To this end, we use *Binary Decision Diagrams (BDDs)* [12, 28] to represent assertions. For a BDD  $B$  and sets of variables  $\mathcal{V}_1, \dots, \mathcal{V}_n$ , we write  $B(\mathcal{V}_1, \dots, \mathcal{V}_n)$  to denote that  $B$  represents an assertion over  $\mathcal{V}_1 \cup \dots \cup \mathcal{V}_n$ . For a state  $s$  over  $\mathcal{V}$ , we write  $s \models B(\mathcal{V})$  to denote that the assertion that  $B$  represents is satisfied by the state  $s$ . BDDs support several *symbolic operations*: conjunction ( $\wedge$ ), disjunction ( $\vee$ ), negation ( $\neg$ ), and extraction of variables using the  $\exists$  and  $\forall$  operators. We measure time complexity of a symbolic algorithm by a worst case #symbolic-operations it performs. A discussion on a rigorous treatment of BDD operations can be found in Appendix A.

**Game Structures and Games.** We follow the notations of [11]. A game structure  $GS = (\mathcal{I}, \mathcal{O}, \theta_{\mathcal{I}}, \theta_{\mathcal{O}}, \rho_{\mathcal{I}}, \rho_{\mathcal{O}})$  defines a turn-based interaction between an *environment* and a *system* players. The input variables  $\mathcal{I}$  and output variables  $\mathcal{O}$  are two disjoint sets of Boolean variables that are controlled by the environment and system, respectively. The environment's *initial assumption*  $\theta_{\mathcal{I}}$  is an assertion over  $\mathcal{I}$ , and the system's *initial guarantee*  $\theta_{\mathcal{O}}$  is an assertion over  $\mathcal{I} \cup \mathcal{O}$ . The environment's *safety assumption*  $\rho_{\mathcal{I}}$  is an assertion over  $\mathcal{I} \cup \mathcal{O} \cup \mathcal{I}'$ , where the interpretation of  $(i_0, o_0, i'_1) \models \rho_{\mathcal{I}}$  is that from state  $(i_0, o_0)$  the environment can assign  $i'_1$  to the input variables. W.l.o.g, we assume that  $\rho_{\mathcal{I}}$  is deadlock free,

i.e., for all  $(i_0, o_0)$  there exists an  $i_1$  s.t.  $(i_0, o_0, i'_1) \models \rho_{\mathcal{I}}$ . Similarly, the system's *safety guarantee*  $\rho_{\mathcal{O}}$  is an assertion over  $\mathcal{I} \cup \mathcal{O} \cup \mathcal{I}' \cup \mathcal{O}'$ , where the interpretation of  $(i_0, o_0, i'_1, o'_1) \models \rho_{\mathcal{O}}$  is that from state  $(i_0, o_0)$  when the environment assigns  $i_1$  to the input variables, the system can assign  $o_1$  to the output variables. Again, w.l.o.g, we assume that  $\rho_{\mathcal{O}}$  is deadlock free, i.e., for all  $(i_0, o_0, i'_1)$  there exists an  $o_1$  s.t.  $(i_0, o_0, i'_1, o'_1) \models \rho_{\mathcal{O}}$ .

A play over  $GS$  progresses by the players taking turns to assign values to their own variables ad infinitum, where the players must satisfy the initial conditions at the start and the safety conditions thereafter. Formally, a *play*  $\pi = s_0, s_1, \dots$  is an infinite sequence of states over  $\mathcal{I} \cup \mathcal{O}$  such that  $s_0 \models \theta_{\mathcal{I}} \wedge \theta_{\mathcal{O}}$  and  $(s_j, s'_{j+1}) \models \rho_{\mathcal{I}} \wedge \rho_{\mathcal{O}}$  for all  $j \geq 0$ . A *play prefix* is either a play or a finite sequence of states that can be extended to a play. Then a *strategy* is a function  $f : (2^{\mathcal{I} \cup \mathcal{O}})^+ \times 2^{\mathcal{I}} \rightarrow 2^{\mathcal{O}}$  such that if  $s_0, \dots, s_m$  is a play prefix,  $(s_m, i') \models \rho_{\mathcal{I}}$  and  $f(s_0, \dots, s_m, i) = o$ , then  $(s_m, i', o') \models \rho_{\mathcal{O}}$ . Intuitively, a strategy directs the system on what to assign to the output variables, depending on the history of a play and the most recent assignment by the environment to the input variables. A play prefix is said to be *consistent with a strategy*  $f$  if for all states  $s_j = (i_j, o_j)$  in that prefix,  $f(s_0, \dots, s_{j-1}, i_j) = o_j$  for all  $j \geq 0$ . A strategy is *memoryless* if it only depends on the last state and the most recent assignment to the input variables. Formally, a *memoryless strategy* is a function  $f : (2^{\mathcal{I} \cup \mathcal{O}}) \times 2^{\mathcal{I}} \rightarrow 2^{\mathcal{O}}$  such that if  $(s_m, i') \models \rho_{\mathcal{I}}$  and  $f(s_m, i') = o$ , then  $(s_m, i', o') \models \rho_{\mathcal{O}}$ .

A *game* is a tuple  $(GS, \varphi)$  where  $GS$  is a game structure over inputs  $\mathcal{I}$  and outputs  $\mathcal{O}$  and  $\varphi$  is an LTL formula over  $\mathcal{I} \cup \mathcal{O}$  called a *winning condition*. A play  $\pi$  is *winning* for the system if  $\pi \models \varphi$ . A strategy  $f$  *wins from state*  $s$  if every play  $\pi$  from  $s$  that is consistent with  $f$  is winning for the system. A strategy  $f$  *wins from*  $S$ , where  $S$  is an assertion over  $\mathcal{I} \cup \mathcal{O}$ , if it wins from every state  $s \models S$ . The *winning region* of the system is the set of states from which it has a winning strategy. A strategy  $f$  is *winning* if for every state  $i \models \theta_{\mathcal{I}}$  there exists a state  $o \in 2^{\mathcal{O}}$  such that  $(i, o) \models \theta_{\mathcal{O}}$  and  $f$  wins from  $(i, o)$ . In this paper, we have the following games that are defined over the following winning conditions.

- *Reachability games*:  $F(\varphi)$  where  $\varphi$  is an assertion over  $\mathcal{I} \cup \mathcal{O}$ .
- *Safety games*:  $G(\varphi)$  where  $\varphi$  is an assertion over  $\mathcal{I} \cup \mathcal{O}$ .
- *Büchi games*:  $GF(\varphi)$  where  $\varphi$  is an assertion over  $\mathcal{I} \cup \mathcal{O}$ .
- *GR(k) games*:  $\bigwedge_{l=1}^k (\bigwedge_{i=1}^{n_l} GF(\varphi_{l,i}) \rightarrow \bigwedge_{j=1}^{m_l} GF(\psi_{l,j}))$  where all  $\varphi_{l,i}$  and  $\psi_{l,j}$  are assertions over  $\mathcal{I} \cup \mathcal{O}$ .

Given a game  $(GS, \varphi)$ , *realizability* is the problem of deciding whether a winning strategy for the system exists, and *synthesis* is the problem of constructing a winning strategy if one exists. We note that a realizability check can be reduced to the identification of the winning region,  $W$ : A winning strategy exists iff for all  $i \models \theta_{\mathcal{I}}$  there exists  $o \in 2^{\mathcal{O}}$  such that  $(i, o) \models \theta_{\mathcal{O}}$  and  $(i, o) \in W$ . Hence, the synthesis problem can be solved by constructing a strategy that wins from  $W$ .

**Game Graphs and Weak Büchi Games.** The *game graph* for a game structure  $GS$  is the directed graph  $(V, E)$  with vertices  $V = 2^{\mathcal{I} \cup \mathcal{O}}$  and edges

$E = \{(s, t) \mid (s, t') \models \rho_{\mathcal{I}} \wedge \rho_{\mathcal{O}}\}$ . Intuitively, vertices are states over  $\mathcal{I}$  and  $\mathcal{O}$ , and edges represent valid transitions between states according to the safety conditions. The game graph can be useful for analyzing the structural properties of a game structure via graph-theoretical properties.

A *finite path* in a directed graph  $(V, E)$  is a sequence  $v_0, \dots, v_n \in V^+$  such that  $(v_j, v_{j+1}) \in E$  for all  $0 \leq j < n$ . An *infinite path*  $v_0, v_1, \dots \in V^\omega$  is similarly defined. A vertex  $u$  is said to be *reachable* from another vertex  $v$  if there is a finite path from  $v$  to  $u$ . A *strongly connected component* (SCC) of a directed graph  $(V, E)$  is a maximal set of vertices within which every vertex is reachable from every other vertex. It is well known that SCCs partition the set of vertices of a directed graph, and that the set of SCCs is partially ordered with respect to reachability. Also note that every infinite path ultimately stays in an SCC.

Let  $(GS, GF\varphi)$  be a game with a Büchi winning condition, and let  $S_0 \dots, S_m$  be the set of SCCs that partition the game graph of  $GS$ . We say that  $(GS, GF\varphi)$  is a *weak Büchi game* if, given the set  $\mathcal{F}$  of states that satisfy the assertion  $\varphi$ , for every SCC  $S_i$ , either  $S_i \subseteq \mathcal{F}$  or  $S_i \cap \mathcal{F} = \emptyset$ . Thus, the SCCs of a weak Büchi game are either *accepting components*, meaning all of its states are contained in  $\mathcal{F}$ , or *non-accepting components*, meaning none of its states is present in  $\mathcal{F}$ . As a consequence, a play in a weak Büchi game is winning for the system if the play ultimately never exits an accepting component. Similarly, a strategy is winning for the system if it can guarantee that every play will ultimately remain inside an accepting component.

### 3 Separated GR( $k$ ) Games

Our framework relies on the core idea of reducing the problem of adapter generation to synthesizing a *Separated GR( $k$ ) game*, which we define in this section. At a high-level, a separated GR( $k$ ) differentiates from a regular GR( $k$ ) game in a separation between input and output variables in both the game structure and winning condition. We show in later sections that the separation of variables leads to algorithmic benefits to the synthesis problem. Formally,

**Definition 1.** A game structure  $GS = (\mathcal{I}, \mathcal{O}, \theta_{\mathcal{I}}, \theta_{\mathcal{O}}, \rho_{\mathcal{I}}, \rho_{\mathcal{O}})$  separates variables over input variables  $\mathcal{I}$  and output variables  $\mathcal{O}$  if:

- The environment’s initial assumption  $\theta_{\mathcal{I}}$  is an assertion over  $\mathcal{I}$  only.
- The system’s initial guarantees  $\theta_{\mathcal{O}}$  is an assertion over  $\mathcal{O}$  only.
- The environment’s safety assumption  $\rho_{\mathcal{I}}$  is an assertion over  $\mathcal{I} \cup \mathcal{I}'$  only.
- The system’s safety guarantee  $\rho_{\mathcal{O}}$  is an assertion over  $\mathcal{O} \cup \mathcal{O}'$  only.

The interpretation of a game structure which separates variables is that the underlying game graph  $(V, E)$  is the product of two distinct directed graphs over disjoint sets of variables:  $G_{\mathcal{I}}$  over the variables  $\mathcal{I} \cup \mathcal{I}'$ , and  $G_{\mathcal{O}}$  over the variables  $\mathcal{O} \cup \mathcal{O}'$ . For  $\mathcal{J} \in \{\mathcal{I}, \mathcal{O}\}$ , the vertices of  $G_{\mathcal{J}}$  correspond to states over  $\mathcal{J}$  and there is an edge between states  $s$  and  $t$  if  $(s, t') \models \rho_{\mathcal{J}}$ .

Next, the notion of separation of variables extends to games with GR( $k$ ) winning conditions as follows:

**Definition 2.** A  $GR(k)$  winning condition  $\varphi$  over  $\mathcal{I} \cup \mathcal{O}$  separates variables w.r.t.  $\mathcal{I}$  and  $\mathcal{O}$  if  $\varphi = \bigwedge_{l=1}^k (\bigwedge_{i=1}^{n_l} \text{GF}(\varphi_{l,i}) \rightarrow \bigwedge_{j=1}^{m_l} \text{GF}(\psi_{l,j}))$  such that each  $\varphi_{l,i}$  is an assertion over  $\mathcal{I}$  and each  $\psi_{l,j}$  is an assertion over  $\mathcal{O}$ .

A *Separated  $GR(k)$  game* is a  $GR(k)$  game  $(GS, \varphi)$  over  $\mathcal{I} \cup \mathcal{O}$  in which both  $GS$  and  $\varphi$  separate variables w.r.t.  $\mathcal{I}$  and  $\mathcal{O}$ .

A major observation is that in a game played over a separated game structure, the actions of the two players are independent: the environment's actions do not limit the system's actions, and vice versa. In later sections we see how this observation leads to algorithmic improvements in solving separated  $GR(k)$  games over a regular  $GR(k)$  game. Specifically, in Section 4 we see how to use Separated  $GR(k)$  games to generate the adapter transducer. In Sections 5 and 6 we discuss algorithms for realizability and synthesis of Separated  $GR(k)$  games.

## 4 From Transducers to Separated $GR(k)$

We describe, using an end-to-end-example, how adapter transducer generation can be reduced to synthesis of Separated  $GR(k)$  games.

We begin with user-provided *Target* and *Adaptee* transducers. These transducers model the behavior of a system that we want to use (*Adaptee*) and the behavior of a system that we want to emulate (*Target*). For example, the transition systems in Figure 1 formulates the following scenario. (1) *Target* is a hardware with three modes that we use, such that the  $U$  (up) and the  $D$  (down) commands send the hardware from mode  $s_0$  to modes  $s_1$  and  $s_2$ , respectively, from which the  $S$  (stay) command keeps the system looping at the chosen mode. (2) *Adaptee* that is a hardware that we *want* to use and also has three modes, but which does not allow the command  $S$  after  $U$ . Instead, it allows a  $D$  command that switches the mode back to  $s_0$ .

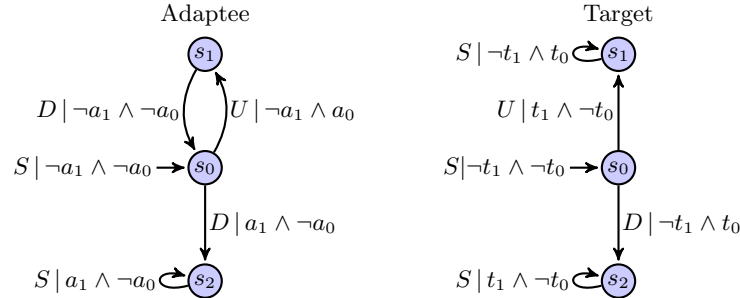


Fig. 1: An example of *Adaptee* and *Target* transducers. In this example, the  $a_i$  and  $t_i$  variables encode the binary representation of the mode being moved to.

The second step is a formulation of the equivalence relation, where we define the type of emulation that we require. In our example we want to maintain the

following property: if *Target* visits a mode  $s_i$  infinitely often for a certain input sequence, then so does  $\text{Adaptee} \circ \text{Adapter}$ . This can be expressed in LTL as:

$$\bigwedge_{i=0}^2 \text{GF}(\text{bin}_t(s_i)) \rightarrow \text{GF}(\text{bin}_a(s_i))$$

where  $\text{bin}_t(s_i)$  denotes the binary representation of mode  $s_i$  using variables  $t_1, t_0$ , and similarly for  $\text{bin}_a(s_i)$  using variables  $a_1, a_0$ . Note that in this example we cannot just synthesize an adapter that cycles through all modes in  $\text{Adaptee} \circ \text{Adapter}$  infinitely often, since the *Adaptee* transducer does not allow that.

As a third step, to generate a separated  $\text{GR}(k)$  game, we translate the *Target* and *Adaptee* transducers to *Input* and *Output* transition systems as depicted, for example, in Figure 2. Since *Adaptee* and *Target* are two separate transducers, each with its own structure, it is natural to model these as two separate transition systems on distinct variables. Thus, the transition systems are produced by the well known projection construction that turns an FST into a FSA that accepts the output language of the transducers [45]. Note that in our setting *Target* is translated to *Input* and *Adaptee* is translated to *Output*. This may appear as a role inversion to readers. We propose it because the role of the controller in our setting is to translate the behavior of *Target* to an equivalent behavior of the *Adaptee*.

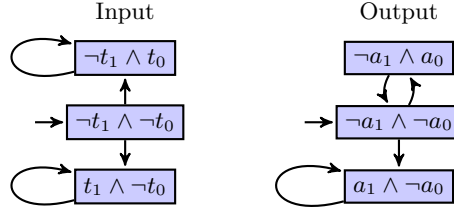


Fig. 2: A direct translation of the *Target* transducer to an *Input* transition system and of the *Adaptee* transducer to an *Output* transition system.

These separate transition systems, together with the specification described above, form a Separated  $\text{GR}(k)$  that, as a fourth step, we can feed to the Separated  $\text{GR}(k)$  synthesis algorithm. The output of the algorithm is a transducer called *Controller*, that maps runs of *Input* to runs of *Output*, as shown, in our example, in Figure 3. This, in fact, connects the output of the *Target* to the output of the *Adaptee*.

As a final step, from the controller we can construct the *Adapter* using the formula  $\text{Adapter} = \text{Adaptee}^{-1} \circ \text{Controller} \circ \text{Target}$ . This means that *Adapter* contains an internal model of the *Target* and of the *Adaptee*. These internal models are used to translate inputs to expected outputs of the adapter, then feed them to the controller, and then feed the output of the controller to the



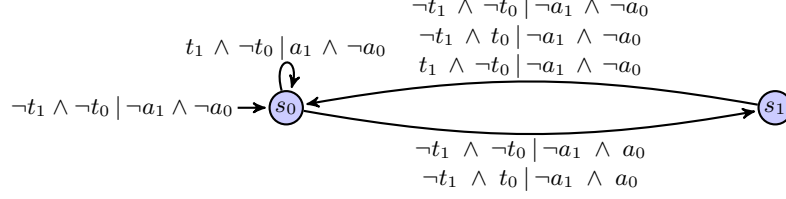


Fig. 3: A controller that reads runs of the *Input* transition system and generates runs of the *Output* transition system such that the specified Separated GR(2) formula is guaranteed to be true.

reverse of *Adaptee* to generate an input to *Adaptee* that emulates the behaviour of *Target*. Note that it is possible to invert transducers symbolically [26].

#### 4.1 Additional Usages of our Technique

We give two more examples to demonstrate uses of Separated GR( $k$ ).

**Cleaning Robots.** This example demonstrates how one can use our technique to fulfill tasks that have not been covered by an execution of an existing transducer. Consider a cleaning robot (the *Target* transducer) that moves along a corridor-shaped house, from room 1 to room  $n$ . The robot follows some plan and accordingly cleans some of the rooms. Our goal is to synthesize a controller that activates a second cleaning robot (the *Adaptee* transducer) that follows the first robot and cleans exactly those rooms left uncleaned. Each robot controls a set of variables indicating which room they are in and which rooms they have cleaned, and additionally the original robot controls a variable indicating whether it is done with its cleaning. Our controller is required to fulfill requirements of the form:  $\text{GF}(\text{done}) \wedge \text{GF}(!\text{in:clean}_i) \rightarrow \text{GF}(\text{out:clean}_i)$ ,  $\text{GF}(\text{done}) \wedge \text{GF}(\text{in:clean}_i) \rightarrow \text{GF}(!\text{out:clean}_i)$ .

**Railway Signalling.** This example demonstrates how one can use our technique to improve the quality of an existing transducer. We consider a junction of  $n$  railways, each equipped with a signal that can be turned on (light in green) or off (light in red). Some railways overlap and thus their signals cannot be turned on simultaneously. We consider an overlapping pattern where railways 1-4 overlap, and similarly 3-6, 5-8, and so on.

An existing system (the *Target* transducer) was programmed to be strictly safe in order to avoid accidents, so it never raises two signals simultaneously. We want to improve the system's performance by synthesizing a controller that reads the assignments that the existing transducer produces and accordingly assign values to the signals in such a way as to produce both safe and *maximal* valuations: the  $i$ th signal is turned on if and only if the signal of every rail that overlaps with the  $i$ th rail is off. Furthermore, we want to maintain liveness

properties of the *Target* system: (1) every signal that is turned on infinitely often by the existing system must be turned on infinitely often by the new system as well, and (2) if a signal is turned on at least once every  $m$  steps (where  $m$  is a parameter of the specification) by the existing system, then the same holds for the new system.

Note that, in terms of the  $\text{GR}(k)$  formula, this example is similar to the “hardware” example that we gave; we want to emulate the *Target*’s execution. The crux of the example lies in its *Adaptee*. Here, unlike in the explanatory example, the *Adaptee* is not a given hardware, but rather a virtual component that the user introduced to improve the *Target* performance. In this case the *Adaptee* produces safe and maximal signals.

## 5 Overview for Solving Separated $\text{GR}(k)$ Games

The adapter generation framework described in Section 4 relies on synthesizing a controller from a separated  $\text{GR}(k)$  game. In this section and the next, we describe how to solve separated  $\text{GR}(k)$  games. This section gives an overview of the algorithm in Section 5.1 and describes a necessary property, called the delay property, in Section 5.2. The delay property is necessary to prove correctness of our synthesis algorithm. Later, Section 6 gives the complete algorithm and proves its correctness.

### 5.1 Algorithm Overview and Intuition

Following Section 3, we are given a Separated  $\text{GR}(k)$  game that consists of a game structure  $GS$  and a winning condition in a  $\text{GR}(k)$  form  $\varphi = \bigwedge_{l=1}^k \varphi_l$ , where  $\varphi_l = \bigwedge_{i=1}^{n_l} \text{GF}(a_{l,i}) \rightarrow \bigwedge_{j=1}^{m_l} \text{GF}(g_{l,j})$ . Let  $G$  be the game graph of  $GS$ . Consider an infinite play  $\pi$  in  $GS$ . Like every infinite path on a finite graph,  $\pi$  eventually stabilizes in an SCC  $S$ . Due to separation of variables, the game graph  $G$  can be decomposed into an input graph  $G_{\mathcal{I}}$  and an output graph  $G_{\mathcal{O}}$ . Then the projection of  $S$  on the inputs is an SCC  $S_{\mathcal{I}}$  in  $G_{\mathcal{I}}$ , and the projection of  $S$  on the outputs is an SCC  $S_{\mathcal{O}}$  in  $G_{\mathcal{O}}$ . The input side of  $\pi$  converges to  $S_{\mathcal{I}}$  whereas the output side  $\pi$  converges to  $S_{\mathcal{O}}$ .

Now, let  $S$  be an SCC with projections  $S_{\mathcal{I}}$  on  $G_{\mathcal{I}}$  and  $S_{\mathcal{O}}$  on  $G_{\mathcal{O}}$ . Then we call  $S$  *accepting* if for *every* constraint  $\varphi_l$ , where  $l \in \{1, \dots, k\}$ , one of the following holds:

**All guarantees hold in  $S$ .** For every  $j \in \{1, \dots, m_l\}$ , there exists  $o \in S_{\mathcal{O}}$  such that  $o \models g_{l,j}$ .

**Some assumption cannot hold in  $S$ .** There exists  $j \in \{1, \dots, n_l\}$  such that for all  $i \in S_{\mathcal{I}}$ ,  $i \not\models a_{l,j}$ .

Then from the definition of an accepting SCC we have the following: a strategy that makes sure that every play converges to an accepting SCC, in which all the relevant guarantee states are visited, is a winning strategy for the system in  $(GS, \varphi)$ . To synthesize such a strategy, we do the following: (i) synthesize a

strategy  $f_B$  for which every play converges to an accepting SCC; (ii) synthesize a strategy  $f_{travel}$  that travels within every accepting SCC, satisfying as many of the  $g_{l,j}$  guarantees as possible. (iii) construct an overall winning strategy  $f$  that works as follows: the system plays  $f_B$  until reaching an accepting SCC  $S$ , then the system switches to  $f_{travel}$  to satisfy as many of the  $g_{l,j}$  guarantees in  $S$  as possible; if the environment moves the play to a non-accepting SCC, the system can start playing  $f_B$  again to reach a different accepting SCC.

The strategy  $f_B$  can be found by synthesizing the weak Büchi game  $(GS, GF(acc))$ , where  $acc$  is the assertion that accepts exactly those states that belong to accepting SCCs (note that  $(GS, GF(acc))$  is a well defined weak Büchi game).  $f_{travel}$  can be constructed by simply finding a path in  $S_{\mathcal{O}}$  that satisfies the maximum number of guarantees.

A complication arises however when switching between  $f_{travel}$  and  $f_B$ , since it is conceivable that while the system is following  $f_{travel}$ , the environment could move to a different SCC that is outside of the winning region of  $f_B$ . Thus, it is not clear that we can combine these strategies to make an overall winning strategy for the system. To show that we can indeed combine both strategies, we need the following property that we call the *delay property*: if  $(i_1, o_1)$  is a state in the winning region of  $f_B$ , and  $(i_2, o_0)$  is a state for which there is a path in  $G_{\mathcal{I}}$  from  $i_1$  to  $i_2$  and a path in  $G_{\mathcal{O}}$  from  $o_0$  to  $o_1$ , then  $(i_2, o_0)$  is also in the winning region of  $f_B$ . We formally state and prove the delay property in Section 5.2. In Section 6 we give details of the construction of  $f_B$ ,  $f_{travel}$  and the use of the delay property to prove correctness of the overall winning strategy  $f$ .

## 5.2 The Delay Property

The delay property essentially says that if an SCC  $S$  is contained in the winning region, and the environment moves from  $S$  unilaterally to a different SCC  $S'$ , then  $S'$  is also in the winning region of the system. In this section, we prove that the Büchi game  $(GS, GF(acc))$  where  $GS = (\mathcal{I}, \mathcal{O}, \theta_{\mathcal{I}}, \theta_{\mathcal{O}}, \rho_{\mathcal{I}}, \rho_{\mathcal{O}})$ , as defined in Section 5.1, satisfies the delay property. Throughout this section, we write  $G_{\mathcal{I}}$  and  $G_{\mathcal{O}}$  to denote the graphs over  $2^{\mathcal{I}}$  and  $2^{\mathcal{O}}$ , respectively, as in Section 5.1. We start with the following lemma that states that the system can still win in spite of a single step delay.

**Lemma 1.** *Let  $i_0, i_1 \in 2^{\mathcal{I}}$  such that  $(i_0, i'_1) \models \rho_{\mathcal{I}}$ , and assume that the system can win from  $(i_0, o_0)$ . Then the system can also win from  $(i_1, o_0)$ .*

*Proof.* Let  $f$  be a winning strategy for the system from  $(i_0, o_0)$ . We construct a winning strategy  $f_d$  from  $(i_1, o_0)$ . Intuitively,  $f_d$  acts from state  $(i_1, o_0)$  as if it were following  $f$  from state  $(i_0, o_0)$ , with a delay of a single step: the input in the current step is used to choose the output in the next step.

We use  $f$  to define  $f_d$  inductively over play prefixes of length  $m \geq 1$ , by setting  $f_d((i_1, o_0), \dots, (i_m, o_{m-1}), i_{m+1}) = f((i_0, o_0), \dots, (i_{m-1}, o_{m-1}), i_m)$ . Note that  $f_d$  is well defined since  $GS$  separates variables: from state  $(i, o)$ , the outputs that can be chosen for the successor state depend only on  $o$ , and not on  $i$ .

Note that by this definition, for every play  $(i_1, o_0), (i_2, o_1), \dots, (i_{m+1}, o_m), \dots$  consistent with  $f_d$ , the play  $(i_0, o_0), (i_1, o_1), \dots, (i_m, o_m), \dots$  is consistent with  $f$ . We remark that we define  $f_d$  only for proving the lemma, and it is *not* part of our solution.

Next, we show that  $f_d$  is winning from  $(i_1, o_0)$ . Take a play  $(i_1, o_0), (i_2, o_1), \dots$ , consistent with  $f_d$ . By the construction,  $(i_0, o_0), (i_1, o_1), \dots$  is consistent with  $f$ . Since this is a play on a weak Büchi game, after some point it must remain in a single SCC  $S$ , say from state  $(i_j, o_j)$ . Since  $f$  is a winning strategy, the SCC  $S$  must be accepting. Then  $o_j, o_{j+1}, \dots$  is an infinite path in the SCC  $S|_{\mathcal{O}}$ , and  $i_j, i_{j+1}, \dots$  is an infinite path in the SCC  $S|_{\mathcal{I}}$ . Consequently,  $(i_1, o_0), (i_2, o_1), \dots$  converges to an SCC  $\hat{S}$  in which  $\hat{S}|_{\mathcal{I}} = S|_{\mathcal{I}}$  and  $\hat{S}|_{\mathcal{O}} = S|_{\mathcal{O}}$ . Since the conditions for an SCC  $D$  to be accepting depend only on the relation between  $D|_{\mathcal{I}}$  and  $D|_{\mathcal{O}}$ , we have that  $\hat{S}$  is accepting since  $S$  is accepting as well.  $\square$

We can now prove the delay property, following by straightforward induction from Lemma 1.

**Theorem 1 (Delay Property Theorem).** *Let  $i_0, \dots, i_n \in (2^{\mathcal{I}})^+$  be a path in  $G_{\mathcal{I}}$ , and for  $m \geq 0$ , let  $o_{-m}, \dots, o_0 \in (2^{\mathcal{O}})^+$  be a path in  $G_{\mathcal{O}}$ . Assume that the system can win from  $(i_0, o_0)$ . Then the system can also win from  $(i_n, o_{-m})$ .*

*Proof.* From  $(i_n, o_{-m})$ , the system can simply ignore the inputs and follow the path in  $G_{\mathcal{O}}$  to  $o_0$ . Let  $(i_{n+m}, o_0)$  be the state at that point in some play. Note that there is a path between  $i_n$  and  $i_{n+m}$ , and therefore there is a path between  $i_0$  and  $i_{n+m}$ . If the system can win from  $(i_0, o_0)$  then by using Lemma 1 in the induction steps, the system can win by induction from  $(i, o_0)$  for all  $i$  such that there is a path in between  $i_0$  and  $i$ . Therefore, the system can win from  $(i_{n+m}, o_0)$ , and by consequence from  $(i_n, o_{-m})$ .  $\square$

A corollary of Theorem 1 is the following statement about the structure of the winning region of the weak Büchi game  $B = (GS, GF(acc))$  as defined in Section 5.1.

**Corollary 1.** *The winning region of  $B$  is a union of SCCs.*

*Proof.* Let  $(i, o)$  be a state in the winning region of  $B$ , let  $(\hat{i}, \hat{o})$  be a state in the same SCC  $S$  of  $(i, o)$ , and let  $S|_{\mathcal{I}}$  and  $S|_{\mathcal{O}}$  be the projections of  $S$  on  $G_{\mathcal{I}}$  and  $G_{\mathcal{O}}$ , respectively. Then there is a path  $i_0, \dots, i_n$  for some  $n \geq 0$  in  $S|_{\mathcal{I}}$  such that  $i_0 = i$  and  $\hat{i} = i_n$ . Similarly, there is a path  $o_{-m}, \dots, o_0$  for some  $m \geq 0$  in  $S|_{\mathcal{O}}$  such that  $\hat{o}_0 = o$  and  $\hat{o} = o_{-m}$ . Then by the delay property of Theorem 1, the vertex  $(\hat{i}, \hat{o}) = (i_n, o_{-m})$  is also in the winning region of  $B$ .  $\square$

We use Theorem 1 and Corollary 1 in the proof of correctness of the overall winning strategy  $f$ , as described in Section 6.2.

## 6 Algorithms for Solving Separated GR( $k$ ) Games

In this section we provide the exact details of our synthesis algorithm for Separated GR( $k$ ) games, as described in Section 5.1. Since constructing  $f_B$  involves defining and solving a weak Büchi game, we first describe these in Section 6.1. We remark that our weak Büchi game synthesis algorithm works for all weak Büchi games, and not just for the special weak Büchi game defined in Section 5.1. Specifically, it works even when the underlying game structure does not separate variables. Next, in Section 6.2, we complete the algorithm construction and describe the correctness of our overall synthesis algorithm. Full proofs of the theorems in this section appear in Appendix B.

### 6.1 Realizability and Synthesis for Weak Büchi Games

We present a symbolic algorithm to solve synthesis of a weak Büchi game. When represented in explicit state-representation, weak Büchi games are known to be solved in linear-time in the size of the game [15, 35]. In this section, we adapt the algorithm from [15, 35] to symbolic state-space representation. For sake of exposition, we give an overview of the algorithm and then present our symbolic modification.

**Overview** Given a weak Büchi game, recall that each SCC in its game graph  $G$  is either an accepting SCC or a non-accepting SCC. The goal is to find the winning regions in the weak Büchi game. This can be done by backward induction on the topological ordering of the SCCs as follows. Let  $(S_0, \dots, S_m)$  be a topological sort of the SCCs in  $G$ .

**Base Case:** Consider all *terminal partitions*, say  $S_j, \dots, S_m$ ; that is, every SCC from which no other SCC is reachable. In this case, plays beginning in a terminal SCC will never leave it. Therefore, all states of terminal SCCs that are accepting are in the winning region of the system and all states of terminal SCCs that are non-accepting are not in the winning region of the environment.

**Induction Step:** Let  $\vec{S} = (S_{i+1}, \dots, S_m)$ , and suppose that the set  $\bigcup \vec{S}$  has been classified into winning regions for the system  $W_{i+1}^s$  and the environment  $W_{i+1}^e$ , respectively. Let  $\vec{S}_{new} = (S_j, S_{j+1}, \dots, S_i)$  be the SCCs from which all edges leaving the SCC lead to an SCC in  $\vec{S}$ . Further, let  $A$  and  $N$  be the unions of all accepting SCCs and all non-accepting SCCs in  $\vec{S}_{new}$ , respectively. Then the basic idea is as follows: The system can win from  $s \in N$  if and only if it can force  $F(W_{i+1}^s)$  from  $s$ . Analogously, the system can win from  $s \in A$  if and only if it can force  $G(A \cup W_{i+1}^s)$  from  $s$ . Hence, by solving these reachability and safety games, we can update  $W_{i+1}^s$  and  $W_{i+1}^e$  into  $W_j^s$  and  $W_j^e$  that partition the larger set  $\bigcup (S_j, \dots, S_m)$  into winning regions for the system and the environment. The winning strategy can be constructed in a standard way as a side-product of the reachability and safety games in each step, see for example [58, 59].

**Symbolic Algorithm for Weak Büchi Games.** Given a weak Büchi game  $B = ((\mathcal{I}, \mathcal{O}, \theta_{\mathcal{I}}, \theta_{\mathcal{O}}, \rho_{\mathcal{I}}, \rho_{\mathcal{O}}), \text{GF}(\text{acc}))$  with BDDs representing  $\theta_{\mathcal{I}}, \theta_{\mathcal{O}}, \rho_{\mathcal{I}}, \rho_{\mathcal{O}}$  and  $\text{acc}$ , our goal is to compute a BDD for the winning region and to synthesize a memoryless winning strategy for the system. The construction follows a fixed-point computation that adapts the inductive procedure described in the overview: In the basis of the fixed point computation, the winning region is the set of accepting terminal SCCs; in the inductive step, the winning region includes winning states by examining SCCs that are higher in the topological ordering on SCCs. In what follows we describe a sequence of BDDs that we construct towards constructing the overall BDD for the winning region. We use the notation  $X$  to denote a set of variables over  $\mathcal{I} \cup \mathcal{O}$ . For the sake of the current construction, memoryless strategies are given in the form of BDDs over  $X, X'$ , for further details on the BDDs constructions refer to Appendix A.

*BDD constructions.* We start by constructing a BDD for a predicate that indicates whether two states in a game structure are present in the same SCC. Let predicate  $\text{Reach}(s, t')$  hold if there is a path from state  $s$  over  $\mathcal{I} \cup \mathcal{O}$  to state  $t$  over  $\mathcal{I} \cup \mathcal{O}$  in the game structure  $GS$ . Similarly, a predicate  $\text{Reach}^{-1}(s, t')$  holds if and only if  $\text{Reach}(t, s')$  holds. BDDs for  $\text{Reach}$  and  $\text{Reach}^{-1}$  can be computed in  $O(N)$  symbolic operations using the transition relation of the game structure. Then, a BDD indicating if two states share the same SCC, is constructed in  $O(N)$  symbolic operations by  $\text{SCC}(X, X') := \text{Reach}(X, X') \wedge \text{Reach}^{-1}(X, X')$ .

Next, we construct a BDD for the union of the terminal SCCs, required by the basis of induction for the construction of the winning region. Let predicate  $\text{Terminal}(s)$  hold if state  $s$  over  $\mathcal{I} \cup \mathcal{O}$  is present in a terminal SCC. Then  $\text{Terminal}(X) := \forall X' : \text{Reach}(X, X') \rightarrow \text{SCC}(X, X')$ . Therefore, given BDDs for  $\text{Reach}$  and  $\text{SCC}$ , the construction of  $\text{Terminal}$  requires  $O(1)$  symbolic operations.

*Computing the Winning Region.* We now describe the fixed-point computation to construct a BDD for the winning region in a weak Büchi game. Let  $\text{Reachability}_{(M,N)}(X)$  denote a BDD generated by solving a reachability game that takes as input a set of source states  $M$  and target states  $N$  and outputs those states in  $M$  from which the system can guarantee to move into  $N$ . Similarly, let  $\text{Safety}_{(M,N)}(X)$  denote a BDD generated by solving a safety game that takes as input a set of source states  $M$  and target states  $N$  and outputs those states in  $M$  from which the system can guarantee that all plays remain inside the set  $N$ . These constructions are standard, details can be found in [25, Chapter 2].

Now, let  $\text{Win}(s)$  denote that state  $s$  over  $\mathcal{I} \cup \mathcal{O}$  is in the winning region. Then,  $\text{Win}(X)$  is the fixed point of the BDD  $\text{Win\_Aux}$  defined below, where the construction essentially follows the high-level algorithm description. The BDD  $\text{Acc}(X)$  represents the formula  $\text{acc}$  encoding the set of accepting states. In addition,  $\text{DC}^i(X)$  is the union  $\bigcup \tilde{S}$  of the Downward-Closed set of SCCs, i.e. the SCCs that have already been classified into winning or not-winning, and  $\text{DC}_{new}^i(X)$  is the union  $\bigcup \tilde{S}_{new}$  of the SCCs in  $\text{DC}^i(X)$  that were not in  $\text{DC}^{i-1}(X)$ . Finally,  $\text{N}^i(X)$  is the subset  $N$  of non-accepting states in  $\text{DC}_{new}^i(X)$ , and  $\text{A}^i(X)$

is the subset  $A$  of accepting states in  $\text{DC}_{\text{new}}^i(X)$ . We then define  $\text{Win\_Aux}$  as follows.

**Base Case.**  $\text{Win\_Aux}^0(X) := \text{Terminal}(X) \wedge \text{Acc}(X)$  and  $\text{DC}^0(X) := \text{Terminal}(X)$

**Inductive Step.**

$$\text{DC}^{i+1}(X) := \forall X' : \text{Reach}(X, X') \rightarrow (\text{SCC}(X, X') \vee \text{DC}^i(X'))$$

$$\text{DC}_{\text{new}}^{i+1}(X) := \text{DC}^{i+1}(X) \setminus \text{DC}^i(X)$$

$$\text{N}^{i+1}(X) := \text{DC}_{\text{new}}^{i+1}(X) \wedge \neg \text{Acc}(X)$$

$$\text{A}^{i+1}(X) := \text{DC}_{\text{new}}^{i+1}(X) \wedge \text{Acc}(X)$$

$$\begin{aligned} \text{Win\_Aux}^{i+1}(X) &:= \text{Win\_Aux}^i(X) \\ &\vee \text{Reachability}_{(\text{N}^{i+1}(X), \text{Win\_Aux}^i(X))}(X) \\ &\vee \text{Safety}_{(\text{A}^{i+1}(X), \text{A}^{i+1}(X) \vee \text{Win\_Aux}^i(X))}(X) \end{aligned}$$

To explain the construction of  $\text{Win}$ , note that a state  $s$  in  $\text{DC}^{i+1}(X)$  is winning in one of these cases: (i)  $s$  is a winning state in  $\text{DC}^i(X)$ . (ii)  $s$  is a non-accepting state in  $\text{DC}^{i+1}(X)$  from which the system can force the play into a winning state in  $\text{DC}^i(X)$ . This set of states can be obtained from  $\text{Reachability}_{(\text{N}^{i+1}(X), \text{Win\_Aux}^i(X))}(X)$ . (iii)  $s$  is an accepting state in  $\text{DC}^{i+1}(X)$  from which the system can guarantee that every play that leaves the accepting SCC moves into a winning state in  $\text{DC}^i(X)$ . This set of states can be obtained from  $\text{Safety}_{(\text{A}^{i+1}(X), \text{A}^{i+1}(X) \vee \text{Win\_Aux}^i(X))}(X)$ .

Finally, to check realizability, construct the BDD  $\forall \mathcal{I}(\text{InitIn}(\mathcal{I}) \rightarrow \exists \mathcal{O}(\text{InitOut}(\mathcal{O}) \wedge \text{Win}(\mathcal{I} \cup \mathcal{O})))$ , where  $\text{InitIn}(\mathcal{I})$  and  $\text{InitOut}(\mathcal{O})$  are BDDs representing  $\theta_{\mathcal{I}}$  and  $\theta_{\mathcal{O}}$ , respectively. This BDD is equal to *true* iff  $B$  is realizable.

The fixed-point computation can be extended in a standard way to also compute a BDD representation  $\text{Fb}(X, X')$  of the winning strategy  $f_B$ , such that  $(s, (i', o')) \models \text{Fb}(X, X')$  iff  $f_B(s, i) = o$ . See Appendix B.1 for details. We then have the following theorem that follows our construction.

**Theorem 2.** *Realizability and synthesis for weak Büchi games can be done in  $O(N)$  symbolic steps.*

*Proof Outline.* The proposed construction symbolically implements the inductive procedure of the explicit algorithm. Hence, it correctly identifies the system's winning region. It remains to show that the algorithm performs  $O(N)$  symbolic operations. First of all, the constructions of  $\text{SCC}$  and  $\text{Terminal}$  take  $O(N)$  symbolic operations collectively. It suffices to show that in the  $i$ -th induction step, solving the reachability and safety games performs  $O(|\text{DC}^{i+1} \setminus \text{DC}^i|)$  operations. This can be proven by a careful analysis of the operations and the sizes of resulting BDDs using standard results on safety and reachability games. Details have been deferred to Appendix B.1.  $\square$

## 6.2 Realizability and Synthesis for Separated $\text{GR}(k)$ Games

We finally make use of the elements obtained so far towards solving synthesis for Separated  $\text{GR}(k)$  games. Our construction follows the overview from Section 5.1. To recall, we describe and construct two auxiliary strategies  $f_B$  and  $f_{\text{travel}}$  and combine them to generate the final strategy  $f$ . We use the delay property theorem from Section 5.2 to prove the correctness of our algorithm.

We are given a Separated  $\text{GR}(k)$  game structure  $GS = (\mathcal{I}, \mathcal{O}, \theta_{\mathcal{I}}, \theta_{\mathcal{O}}, \rho_{\mathcal{I}}, \rho_{\mathcal{O}})$  and a winning condition  $\varphi = \bigwedge_{l=1}^k \varphi_l$ , where  $\varphi_l = \bigwedge_{i=1}^{n_l} \text{GF}(a_{l,i}) \rightarrow \bigwedge_{j=1}^{m_l} \text{GF}(g_{l,j})$ . We first represent  $GS$  and  $\varphi$  as BDDs by standard means. We then define and construct the following.

*Constructing  $f_B$ .* Auxiliary strategy  $f_B$  is the winning strategy of the system player in a weak Büchi game constructed from the separated  $\text{GR}(k)$  game. To construct a weak Büchi game, we first construct, in  $O(|\varphi| + N)$  symbolic operations, a BDD  $\text{Acc}(\mathcal{I} \cup \mathcal{O})$  that describes the set of accepting states. The construction is standard, see Lemma 5 in Appendix B.2 for details. Next, let  $\text{acc}$  be the assertion represented by  $\text{Acc}$  (the assertion defined in Section 5.1). Then the Weak Büchi game is  $B = (GS, \text{GF}(\text{acc}))$ . Finally, we construct  $f_B$  as the winning strategy of  $B$ , following Section 6.1 and Section B.1.

*Constructing  $f_{\text{travel}}$ .* For the construction of  $f_{\text{travel}}$ , we arbitrarily order all guarantees that appear in our  $\text{GR}(k)$  formula:  $\text{gar}_0, \dots, \text{gar}_{m-1}$ . For each guarantee  $\text{gar}_j$ , we construct a reachability strategy  $f_{r(j)}$  that, when applied inside an SCC  $S_{\mathcal{O}}$  in the output game graph  $G_{\mathcal{O}}$ , moves towards a state that satisfies  $\text{gar}_j$  without ever leaving  $S_{\mathcal{O}}$ . In case no such state exists in  $S_{\mathcal{O}}$ ,  $f_{r(j)}$  returns a distinguished value  $\perp$ . Note that this strategy can entirely ignore the inputs. We equip  $f_{\text{travel}}$  with a memory variable  $\text{mem}$  that stores values from  $\{0, \dots, m-1\}$ . Then  $f_{\text{travel}}(s, i)$  is operated as follows: for  $\text{mem}, \text{mem}+1, \dots$  we find the first  $\text{mem}+j \pmod{m}$  such that the SCC of  $s$  includes a  $\text{gar}_j$ -state, and activate  $f_{r(\text{mem}+j)}$  to reach such state. If no guarantees can be satisfied in  $S$ , we just return an arbitrary output to stay in  $S_{\mathcal{O}}$ . The construction of  $f_{\text{travel}}$  requires  $O(|\varphi|N)$  symbolic BDD-operations as we need to construct  $m$  reachability strategies (clearly,  $m \leq |\varphi|$ ).

*Constructing the overall strategy  $f$ .* Finally, we interleave the strategies  $f_B$  and  $f_{\text{travel}}$  into a single strategy  $f$  as follows: given a state  $s$  and an input  $i$ , if  $s \models \text{Acc}(X)$  (that is, if  $s$  is an accepting state), then set  $f(s, i) = f_{\text{travel}}(s, i)$ ; otherwise set  $f(s, i) = f_B(s, i)$ . Whenever  $f$  switches from  $f_B$  to  $f_{\text{travel}}$ , the memory variable  $\text{mem}$  is reset to 0. The next lemma proves that if  $f_B$  is winning then so is  $f$ .

**Lemma 2.** *If  $f_B$  is a winning strategy for the weak Büchi game  $B = (GS, \text{GF}(\text{acc}))$ , then  $f$  is a winning strategy for the Separated  $\text{GR}(k)$  game  $(GS, \varphi)$ .*



*Proof.* Since  $f_B$  is a winning strategy, then for every initial input  $i \models \theta_{\mathcal{I}}$  there is an initial output  $o \models \theta_{\mathcal{O}}$  such that  $(i, o)$  is in the winning region of  $GS$ . We show that playing  $f$  always keeps the play in the winning region of  $GS$ , and therefore the play eventually converges to an accepting SCC. Once this happens, following  $f_{travel}$  guarantees that  $\varphi$  is satisfied. We know that as long as the play is in the winning region of  $B$ , following  $f_B$  will keep it inside the winning region. Therefore, when we switch from  $f_B$  to  $f_{travel}$  we must be inside the winning region and, by definition of  $f$ , in some accepting SCC  $S$ . Then  $f_{travel}$  makes sure that as long as the environment remains in  $S|_{\mathcal{I}}$ , the projection of  $S$  over the inputs, the system remains in  $S|_{\mathcal{O}}$ , the projection of  $S$  over the output. Thus all in all the play remains in the winning region of  $S$ .

Therefore, the only way that the play can leave the winning region is if, when the system is in a state  $(i_0, o_0)$  and chooses some output  $o_{-m}$  according to  $f_{travel}$ , the environment chooses input  $i_n$  such that the play leaves  $S$  and moves to a state  $(i_n, o_{-m})$  in a different SCC of  $G$ . Note, however, that in this case there is a path from  $i_0$  to  $i_n$  and a path from  $o_{-m}$  to  $o_0$  (since by construction  $f_{travel}$  remains in the same SCC in  $G_{\mathcal{O}}$ ). Since  $(i_0, o_0)$  is in the winning region, by Theorem 1 we have that  $(i_n, o_{-m})$  is in the winning region as well.  $\square$

**Final Results.** Given Lemma 2, we can obtain our final results on synthesis and realizability of Separated  $GR(k)$  games, as follows. Given a Separated  $GR(k)$  game  $(GS, \varphi)$ , construct  $acc$  and solve the weak Büchi game  $(GS, GF(acc))$ . Then construct  $f_B$ ,  $f_{travel}$  and  $f$  as described above. If realizable, then  $f_B$  is a winning strategy and from Lemma 2 we have that  $f$  is a winning strategy for  $(GS, \varphi)$ . If  $(GS, GF(acc))$  is unrealizable, then the environment can force every play to converge to a non-accepting SCC. Since the  $GR(k)$  winning condition cannot be satisfied from a non-accepting SCC,  $(GS, \varphi)$  is also not realizable. Thus we have the following theorem, see Appendix B.2 for details.

**Theorem 3.** *Realizability for separated  $GR(k)$  games can be reduced to realizability of weak Büchi games.*

The final result on solving Separated  $GR(k)$  games is as follows:

**Theorem 4.** *Let  $(GS, \varphi)$  be a separated  $GR(k)$  game over the input/output variables  $\mathcal{I}$  and  $\mathcal{O}$ , respectively. Then, the realizability and synthesis problems for  $(GS, \varphi)$  are solved in  $O(|\varphi| + N)$  and  $O(|\varphi|N)$  symbolic operations, respectively, where  $N = |2^{\mathcal{I} \cup \mathcal{O}}|$ .*

*Proof.* Following Lemma 2 and Theorem 3, it is left to analyze the number of symbolic operations for constructing  $f_B$  and then  $f$ . In symbolic operations, constructing  $acc$  takes  $O(|\varphi| + N)$ , and computing the winning region  $W$  for  $(GS, GF(acc))$  takes  $O(N)$ . Checking realizability can be done by checking if for every initial input  $i$  there is an initial output  $o$  such that  $(i, o) \in W$ , which takes  $O(1)$ . The winning strategy  $f_B$  can be computed in the process of computing  $W$ , taking the same number of operations (see Appendix B.1 for details). Finally,

constructing  $f_{travel}$  takes  $O((\#gars)N) \leq O(|\varphi|N)$ , where  $gars$  are all guarantees  $\text{GF}(g_{i,\ell})$  that appear in  $\varphi$ . Therefore, constructing  $f$  takes  $O(|\varphi|N)$  symbolic operations in total.  $\square$

This is an improvement over the complexity of  $\text{GR}(k)$  games, in general [49].

## 7 Implementation and Evaluation

We have implemented our Separated  $\text{GR}(k)$  framework for realizability and synthesis in a prototype tool  $\text{SGR}(k)$ . The tool implements our symbolic algorithm using the CUDD [56] package for BDD manipulation. Our tool is evaluated on a suite of benchmarks created from the examples described in Section 4.

**Benchmark Suite.** We have created a suite of parametric benchmarks from the three examples described in Section 4. Our suite consists of 38 realizable specifications. The parametric versions of the examples are described here.

The *multi-mode hardware* example is a generalization of the example presented at the beginning of Section 4. It is parameterized by the number of bits  $n$  and has  $2^n$  modes. The *Target* can move from mode 0 to any mode and stay there, while the *Adaptee* can only move from mode 0 to odd-numbered modes, and up and down between modes  $2i$  and  $2i + 1$ . The specification consists of  $2n$  variables. We generate 10 such benchmarks with  $n \in \{1, \dots, 10\}$ .

The *cleaning robots* example is parameterized in the number of rooms. For a scenario with  $n$  rooms, the specification is written over  $4n + 1$  variables. We create 10 such benchmarks with  $n \in \{1 \dots, 10\}$ .

The *railways signalling* example consists of two parameters: a junction of  $n$  railways and the frequency parameter  $m$ . With parameters  $n$  and  $m$ , the specification consists of  $(2 + 2\lceil \log m \rceil)n$  variables. We generate 18 benchmarks with  $n \in \{2, \dots, 10\}$  and  $m \in \{2, 3\}$ .

**Experimental Setup and Methodology.** We evaluate our tool against Strix [1, 38, 43], the current state-of-the-art tool for LTL synthesis and SYNT-COMP 2020 winner of 3 out of 4 tracks [2]. In order to run our benchmarks on Strix, we transform the benchmarks (a game structure and a winning condition) into an LTL formula that characterizes the same winning plays using the strict semantics from [27]. To the best of our knowledge, there is no other synthesis/realizability tool that operates on  $\text{GR}(k)$  specifications.

We compare the running time for checking realizability. For this, we compare the runtime of realizability checks of each benchmark on both tools. Every benchmark is tested 10 times on both tools. We do this to account for the randomness introduced during BDD construction due to the automatic variable ordering by CUDD. For each benchmark we evaluate (a). the number of executions on which the tools terminate and (b). the mean running time over 10 executions.

All experiments were executed on a single node of a high-performance computer cluster consisting of an Intel Xeon processor running at 2.6 GHz with 32GB of memory with a timeout of 10 mins.

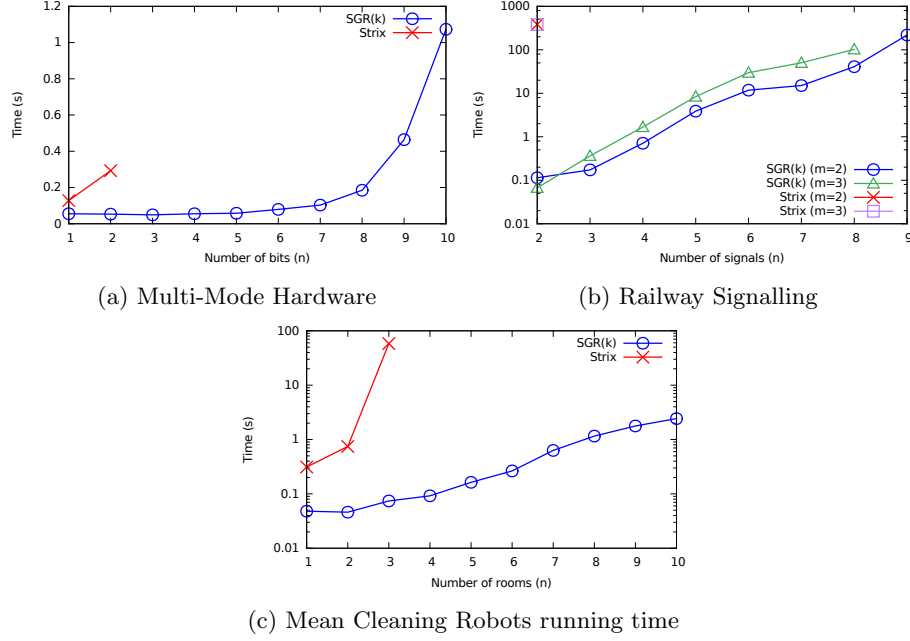


Fig. 4: Mean running time for different classes of benchmarks.

**Observations and Inferences.** Our experiments clearly demonstrate the scalability and efficiency of our tool in solving Separated  $\text{GR}(k)$  formulas.

Figure 4 plots the mean running time for the three benchmarks. We further report the mean values in Table 1. The table rows refer to the benchmarks we examine, and the columns refer to the value of the parameter  $n$ . As an example, for the specification  $\text{Cleaning}(3)$ ,  $\text{SGR}(k)$ 's mean running time is 0.07 sec. (row titled  $\text{Cleaning}(n); \text{SGR}(k)$ , column titled 3) and Strix's median realizability check running time is 58.3 sec. (row titled  $\text{Cleaning}(n); \text{Strix}$ , column titled 4). Cells reading 'TO' indicate experiments reached a timeout.

$n$		1	2	3	4	5	6	7	8	9	10
MultiMode( $n$ )	SGR( $k$ )	0.06	0.05	0.05	0.06	0.06	0.08	0.1	0.19	0.46	1.07
	Strix	0.13	0.29	TO	TO	TO	TO	TO	TO	TO	TO
Cleaning( $n$ )	SGR( $k$ )	0.05	0.05	0.07	0.09	0.16	0.26	0.63	1.16	1.78	2.43
	Strix	0.31	0.75	58.3	TO	TO	TO	TO	TO	TO	TO
Railways( $n, 2$ )	SGR( $k$ )	-	0.11	0.17	0.71	3.88	11.8	15.1	40.8	219	TO
	Strix	-	382	TO	TO	TO	TO	TO	TO	TO	TO
Railways( $n, 3$ )	SGR( $k$ )	-	0.07	0.36	1.67	8.39	29.8	50.3	102	TO	TO
	Strix	-	381	TO	TO	TO	TO	TO	TO	TO	TO

Table 1: Mean realizability check running times (sec.)

The results show that our tool solves a significantly larger number of benchmarks than **Strix**. On the few benchmarks which **Strix** solves, our tool outperforms it by several orders of magnitude. Although the running time may vary depending on the automatic variable ordering chosen by CUDD, we do not believe it would vary enough to significantly change the results. Specifically, we calculated the 99% confidence interval for our results, and validated that for all data points our tool’s entire interval lies below the entire interval for **Strix**.

Only three benchmarks were unsolvable by our tool (in the sense that the majority of the 10 executions timed out). The three benchmarks are the railway signal examples with  $(n = 10, m = 2)$ ,  $(n = 9, m = 3)$ , and  $(n = 10, m = 3)$ . These benchmarks consist of a large number of variables (54, 40, and 60, respectively), making them particularly challenging. All executions of the remaining benchmarks were solved in less than 4 mins by our tool.

We also examined the number of solved executions per benchmark. Our tool solved all 10 executions for 35 out of 38 benchmarks. These are the 35 benchmarks that appear as solved in Figure 4. For the railway signalling benchmark with  $(n = 10, m = 2)$ , our tool solved 2 out of 10 executions. In contrast, **Strix** was not able to solve even one execution for 31 out of 38 benchmarks. Even increasing the timeout to 8hrs only allowed **Strix** to solve a single additional benchmark. In total, **Strix** and our tool verified realizability of 7 benchmarks and 36 out of 38 benchmarks, respectively.

In summary, our experiments demonstrate that our tool is able to solve specifications which are challenging for existing tools.

## 8 Related Work

The Adapter design pattern was introduced in [23], and has been used in many software contexts since. Our interpretation of the pattern is inspired by automata based description of the pattern proposed by Pedrazzini [48]. We reformulated the problem as synthesis of reactive controllers that compose with existing systems to achieve a temporal specification. This is an active area of research [4, 8, 9, 16, 18, 22]. Our work differs from existing frameworks in its variables separation feature. *Shield synthesis* is a notable similar problem in which a synthesized controller corrects safety violations of an existing controller [30]. In contrast, our problem is mostly concerned about liveness adaptation.

Reactive synthesis of LTL winning conditions is 2EXPTIME complete in the size of the formula [51], making it difficult to scale for applications. An approach to overcome the computational barrier has been to investigate fragments and variants of LTL with lower complexity for synthesis [5, 17, 20, 37, 60]. The  $\text{GR}(k)$  is one such fragment [11]. It offers a balance between efficiency and expressiveness.  $\text{GR}(k)$  games are known to be efficient as they are solved in exponential time in the number of conjunctions  $k$  rather than exponential in the state-space [49]. Several studies have also shown they are highly expressive. As evidence, all properties expressed by deterministic Büchi automata (DBA) can be expressed in  $\text{GR}(k)$  [20]. A study of commonly appearing LTL patterns has

shown that 52 of 55 patterns are DBA properties [19, 40]. DBA properties have also been identified as common patterns in robotics applications [42].

Finally, Separated  $\text{GR}(k)$  games exhibit the *delay property*. Intuitively, this property means that the system can win even after delaying its action for a finite amount of time while ignoring the environment before “catching up” with the environment. While this is reminiscent of asynchrony in reactive systems [7, 52, 55], a further exploration of relations between asynchrony and the delay property is required.

## 9 Conclusion

This paper presents a reactive systems-based model of the adapter design pattern. We model the adapters as transducers and reduce the problem of finding an *Adapter* transducer for a given *Adaptee* and *Target* systems, to the problem of synthesizing strategies for Separated  $\text{GR}(k)$  games. Through an analysis of theoretical complexity and algorithmic performance, we show that realizability and synthesis of Separated  $\text{GR}(k)$  games is efficient and scalable. Furthermore, by outperforming Strix, an existing state-of-the-art synthesis tool, we show that algorithms for the Separated  $\text{GR}(k)$  class of specifications add value to the portfolio of reactive synthesis tools.

The benefits of separation of input and output variables were previously shown in the context of Boolean Functional Synthesis [14]. Through this work, we showed that the separation leads to practically viable solutions even in the context of temporal reactive synthesis, more specifically when encoding the types of equivalence relations that appear in reactive adaptation, where properties of runs of the first system are compared to properties of runs of the other. Since the systems may be loosely coupled, i.e., they may not run on the same clock, specifications that impose joint temporal constraints on the two systems may not be realizable. Thus, our proposition to use the type of equivalence that separated  $\text{GR}(k)$  formulas allow, gives users the power needed for comparing the *overall behaviors* of the systems while allowing realizability and efficient synthesis.

The results presented in this paper encourage future studies on the separation of variables in a broader context. For instance, we could reason about variants of the adapter design pattern that do not separate variables all the way through. That is to say, variants that translate to more general  $\text{GR}(k)$  specifications in which the separation appears in the input and output systems but not in the specification itself. One could further study the notion of separation of variables in more the general LTL specifications. Another direction is to consider systems that gets two types of input: from the existing system (i.e. the *Target*) as well as from an environment. We believe that these future directions would enable the development of tools for synthesis from temporal specifications with a focus on expressing realistic applications as well as ensuring scalability and efficiency for practical needs.

**Acknowledgements** We thank Supratik Chakraborty and Dana Fisman for their inputs at various stages of the project. This work is supported in part by NSF grant 2030859 to the CRA for the CIFellows Project, NSF grants IIS-1527668, CCF-1704883, IIS-1830549, and an award from the Maryland Procurement Office. It was also supported by ISF grant 2714/19 and by the Lynn and William Frankel Center for Computer Science.

## Bibliography

- [1] Strix Website. <https://strix.model.in.tum.de/>
- [2] The Reactive Synthesis Competition - SYNTCOMP 2020 Results. <http://www.syntcomp.org/syntcomp-2020-results/>, accessed: 2021-05-27
- [3] de Alfaro, L., Henzinger, T.A.: Concurrent omega-regular games. In: Proc. of LICS (2000)
- [4] Alur, R., Moarref, S., Topcu, U.: Compositional synthesis of reactive controllers for multi-agent systems. In: Proc. of CAV (2016)
- [5] Amram, G., Maoz, S., Pistiner, O.: GR(1)\*: GR(1) specifications extended with existential guarantees. In: Proc. of FM (2019)
- [6] Baier, C., Katoen, J.: Principles of model checking. MIT Press (2008)
- [7] Bansal, S., Namjoshi, K.S., Sa’ar, Y.: Synthesis of asynchronous reactive programs from temporal specifications. In: Proc. of CAV (2018)
- [8] Bansal, S., Namjoshi, K.S., Sa’ar, Y.: Synthesis of coordination programs from linear temporal specifications. Proc. of POPL (2019)
- [9] Berardi, D., Calvanese, D., De Giacomo, G., Lenzerini, M., Mecella, M.: Automatic composition of e-services that export their behavior. In: International conference on service-oriented computing (2003)
- [10] Bloem, R., Galler, S.J., Jobstmann, B., Piterman, N., Pnueli, A., Weiglhofer, M.: Interactive presentation: Automatic hardware synthesis from specifications: a case study. In: Lauwereins, R., Madsen, J. (eds.) Proc. of DATE (2007)
- [11] Bloem, R., Jobstmann, B., Piterman, N., Pnueli, A., Sa’ar, Y.: Synthesis of reactive(1) designs. J. Comput. Syst. Sci. **78**(3), 911–938 (2012)
- [12] Bryant, R.E.: Graph-based algorithms for boolean function manipulation. IEEE Trans. Computers **35**(8), 677–691 (1986)
- [13] Bryant, R.E.: Symbolic boolean manipulation with ordered binary-decision diagrams. ACM Comput. Surv. **24**(3), 293–318 (1992)
- [14] Chakraborty, S., Fried, D., Tabajara, L.M., Vardi, M.Y.: Functional synthesis via input-output separation. In: Proc. of FMCAD (2018)
- [15] Chatterjee, K.: Linear time algorithm for weak parity games. CoRR **abs/0805.1391** (2008), <http://arxiv.org/abs/0805.1391>
- [16] Ciolek, D., Braberman, V., D’Ippolito, N., Piterman, N., Uchitel, S.: Interaction models and automated control under partial observable environments. IEEE Transactions on Software Engineering **43**(1), 19–33 (2016)
- [17] De Giacomo, G., Vardi, M.Y.: Linear temporal logic and linear dynamic logic on finite traces. In: Proc. of IJCAI (2013)
- [18] D’ippolito, N., Braberman, V., Piterman, N., Uchitel, S.: Synthesizing nonanomalous event-based controllers for liveness goals. ACM Transactions on Software Engineering and Methodology (TOSEM) **22**(1), 1–36 (2013)
- [19] Dwyer, M.B., Avrunin, G.S., Corbett, J.C.: Patterns in property specifications for finite-state verification. In: Boehm, B.W., Garlan, D., Kramer, J. (eds.) Proc. of ICSE (1999)

- [20] Ehlers, R.: Generalized rabin(1) synthesis with applications to robust system synthesis. In: Bobaru, M.G., Havelund, K., Holzmann, G.J., Joshi, R. (eds.) Proc. of NASA-FM (2011)
- [21] Fisman, D., Kupferman, O.: Reasoning about finite-state switched systems. In: Haifa Verification Conference. pp. 71–86 (2009)
- [22] Fried, D., Legay, A., Ouaknine, J., Vardi, M.Y.: Sequential relational decomposition. In: Proc. of LICS (2018)
- [23] Gamma, E.: Design patterns: elements of reusable object-oriented software. Pearson Education India (1995)
- [24] Grabmayer, C., Endrullis, J., Hendriks, D., Klop, J.W., Moss, L.S.: Automatic sequences and zip-specifications. In: Proc. of LICS (2012)
- [25] Grädel, E., Thomas, W., Wilke, T. (eds.): Automata, Logics, and Infinite Games: A Guide to Current Research (2002)
- [26] Hu, Q., D’Antoni, L.: Automatic program inversion using symbolic transducers. SIGPLAN Not. p. 376–389 (Jun 2017)
- [27] Jacobs, S., Klein, F., Schirmer, S.: A high-level LTL synthesis format: TLSF v1.1. In: Proc. of SYNT (2016)
- [28] Jr., S.B.A.: Binary decision diagrams. IEEE Trans. Computers **27**(6), 509–516 (1978)
- [29] Kocher, P., Horn, J., Fogh, A., , Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., Mangard, S., Prescher, T., Schwarz, M., Yarom, Y.: Spectre attacks: Exploiting speculative execution. In: Proc. of (S&P’19) (2019)
- [30] Könighofer, B., Alshiekh, M., Bloem, R., Humphrey, L.R., Könighofer, R., Topcu, U., Wang, C.: Shield synthesis. Formal Methods Syst. Des. **51**(2), 332–361 (2017)
- [31] Koruyeh, E.M., Khasawneh, K.N., Song, C., Abu-Ghazaleh, N.: Spectre returns! speculation attacks using the return stack buffer. In: Proc. of USENIX Workshop on Offensive Technologies (WOOT) (2018)
- [32] Kress-Gazit, H., Fainekos, G.E., Pappas, G.J.: Temporal-logic-based reactive mission and motion planning. IEEE Trans. Robotics (2009)
- [33] Lind-Nielsen, J.: BuDDy - a Binary Decision Diagram Package. <http://vlsicad.eecs.umich.edu/BK/Slots/cache/www.itu.dk/research/buddy/>
- [34] Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Fogh, A., Horn, J., Mangard, S., Kocher, P., Genkin, D., Yarom, Y., Hamburg, M.: Meltdown: Reading kernel memory from user space. In: Proc. of USENIX (2018)
- [35] Löding, C., Thomas, W.: Alternating automata and logics over infinite words. In: van Leeuwen, J., Watanabe, O., Hagiya, M., Mosses, P.D., Ito, T. (eds.) Theoretical Computer Science, Exploring New Frontiers of Theoretical Informatics, International Conference IFIP. vol. 1872, pp. 521–535. Springer (2000)
- [36] Lothaire, M.: Applied combinatorics on words, vol. 105. Cambridge University Press (2005)
- [37] Lustig, Y., Vardi, M.Y.: Synthesis from component libraries. In: Proc. of FoSSaCS (2009)



- [38] Luttenberger, M., Meyer, P.J., Sickert, S.: Practical synthesis of reactive systems from LTL specifications via parity games. *Acta Informatica* **57**(1-2), 3–36 (2020)
- [39] Maoz, S., Ringert, J.O.: Synthesizing a lego forklift controller in GR(1): A case study. In: *Proc. of SYNT* (2015)
- [40] Maoz, S., Ringert, J.O.: GR(1) synthesis for LTL specification patterns. In: Knoop, J., Zdun, U. (eds.) *Software Engineering* (2016)
- [41] Martin, D.A.: Borel determinacy. *Annals of Mathematics* pp. 363–371 (1975)
- [42] Menghi, C., Tsigkanos, C., Pelliccione, P., Ghezzi, C., Berger, T.: Specification patterns for robotic missions. *IEEE Transactions on Software Engineering* pp. 1–1 (2019)
- [43] Meyer, P.J., Sickert, S., Luttenberger, M.: Strix: Explicit reactive synthesis strikes back! In: Chockler, H., Weissenbacher, G. (eds.) *Proc. of CAV* (2018)
- [44] Milvang-Jensen, K., Hu, A.J.: BDDNOW: A parallel BDD package. In: *Proc. of FMCAD* (1998)
- [45] Mohri, M.: Finite-state transducers in language and speech processing. *Comput. Linguist.* **23**(2), 269–311 (Jun 1997)
- [46] Ozay, N., Topcu, U., Murray, R.M.: Distributed power allocation for vehicle management systems. In: *Proc. of CDC-ECC* (2011)
- [47] Ozay, N., Topcu, U., Murray, R.M., Wongpiromsarn, T.: Distributed synthesis of control protocols for smart camera networks. In: *Proc. of ICCPS* (2011)
- [48] Pedrazzini, S.: The finite state automata’s design patterns. In: Champarnaud, J.M., Ziadi, D., Maurel, D. (eds.) *Automata Implementation*. pp. 213–219. Springer Berlin Heidelberg, Berlin, Heidelberg (1999)
- [49] Piterman, N., Pnueli, A.: Faster solutions of rabin and streett games. In: *Proc. of LICS* (2006)
- [50] Pnueli, A.: The temporal logic of programs. In: *Proc. of FOCS* (1977)
- [51] Pnueli, A., Rosner, R.: On the synthesis of a reactive module. In: *Proc. of POPL* (1989)
- [52] Pnueli, A., Rosner, R.: On the synthesis of an asynchronous reactive module. In: Ausiello, G., Dezani-Ciancaglini, M., Rocca, S.R.D. (eds.) *Proc. of ICALP* (1989)
- [53] Ryzhyk, L., Walker, A.: Developing a practical reactive synthesis tool: Experience and lessons learned. In: Piskac, R., Dimitrova, R. (eds.) *Proc. of SYNT* (2016)
- [54] Sanghavi, J.V., Ranjan, R.K., Brayton, R.K., Sangiovanni-Vincentelli, A.: High performance bdd package by exploiting memory hierarchy. In: *Proc. of DATE* (1996)
- [55] Schewe, S., Finkbeiner, B.: Synthesis of asynchronous systems. In: Puebla, G. (ed.) *Proc. of LOPSTR* (2006)
- [56] Somenzi, F.: CUDD: CU Decision Diagram Package Release 3.0.0. <http://vlsi.colorado.edu/~fabio/CUDD/cudd.pdf> (2015)
- [57] Yang, B.: ABCD. <http://fmv.jku.at/abcd/>

- [58] Zhu, S., Tabajara, L.M., Li, J., Pu, G., Vardi, M.Y.: A symbolic approach to safety ltl synthesis. In: Proc. of HVC (2017)
- [59] Zhu, S., Tabajara, L.M., Li, J., Pu, G., Vardi, M.Y.: Symbolic ltlf synthesis. In: Proc. of IJCAI (2017)
- [60] Zielonka, W.: Infinite games on finitely coloured graphs with applications to automata on infinite trees. Theor. Comput. Sci. **200**(1-2), 135–183 (1998)

## A Binary Decision Diagrams

A *Binary Decision Diagram* (BDD) [12, 28] is a DAG representation of an assertion. The non-leaves BDD nodes are labeled with variable names, the BDD arrows are labeled variable valuations, and BDD leaves with *true/false*. BDDs are considered a useful representation as they support Boolean operations and further satisfaction queries that can be computed efficiently [13]. Various professional tools that implement BDDs exist e.g. [33, 44, 54, 56, 57].

We say that a BDD  $B$  is over  $\mathcal{V}_1, \dots, \mathcal{V}_n$ , if it represents an assertion over  $\mathcal{V}_1 \cup \dots \cup \mathcal{V}_n$ , and write  $B(\mathcal{V}_1, \dots, \mathcal{V}_n)$ . For a BDD  $B(\mathcal{V}_1, \dots, \mathcal{V}_n)$  and states  $s_1, \dots, s_n$  over  $\mathcal{V}_1, \dots, \mathcal{V}_n$ , respectively, we write  $(s_1, \dots, s_n) \models B(\mathcal{V}_1, \dots, \mathcal{V}_n)$  if the assertion that  $B(\mathcal{V}_1, \dots, \mathcal{V}_n)$  represents is evaluated to *true* by the states  $s_1, \dots, s_n$ . For a set of variables  $\mathcal{V}$ , we write  $\mathcal{V} = \mathcal{V}'$  to denote the BDD that represents the assertion  $\bigwedge_{v \in \mathcal{V}} (v = v')$ . We also employ the following *symbolic operations*:

1. Boolean operations over BDDs:  $\neg, \vee, \wedge, \rightarrow$  with their standard meaning.
2. For a BDD  $B(\mathcal{V}_1, \mathcal{V}_2)$ , the BDD  $C(\mathcal{V}_1) := \exists \mathcal{V}_2 (B(\mathcal{V}_1, \mathcal{V}_2))$  satisfies the following: For  $s_1 \in 2^{\mathcal{V}_1}$ ,  $s_1 \models C(\mathcal{V}_1)$  if there exists  $s_2 \in 2^{\mathcal{V}_2}$  such that  $(s_1, s_2) \models B(\mathcal{V}_1, \mathcal{V}_2)$ .
3. Similarly,  $C(\mathcal{V}_1) := \forall \mathcal{V}_2 (B(\mathcal{V}_1, \mathcal{V}_2))$  satisfies: For  $s_1 \in 2^{\mathcal{V}_1}$ ,  $s_1 \models C(\mathcal{V}_1)$  if for all  $s_2 \in 2^{\mathcal{V}_2}$ ,  $(s_1, s_2) \models B(\mathcal{V}_1, \mathcal{V}_2)$ .

We use BDDs to model sets (e.g. winning regions) in a straightforward manner i.e.  $B(\mathcal{V})$  represent  $\{s \in 2^{\mathcal{V}} : s \models B(\mathcal{V})\}$ . We may also use BDDs to represent memoryless strategies as follows:  $F(\mathcal{I}, \mathcal{O}, \mathcal{I}', \mathcal{O}')$  represents the memoryless strategy by  $f(s, i) = o$  iff  $(s, i', o') \models F(\mathcal{I}, \mathcal{O}, \mathcal{I}', \mathcal{O}')$ . The paper presents symbolic constructions of BDDs. Time of such symbolic algorithms is measured in #symbolic-operations performed.

## B Proofs for Section 6

We turn to prove Theorems 2, 3 and 4, given in Section 6. Throughout the appendix, we use the fact that  $\omega$ -regular games are *determined* [25, 41]. That is, for each game with an  $\omega$ -regular winning condition and a state  $s$ , either the system has a winning strategy from  $s$ , or the environment has a spoiling strategy from  $s$ : A strategy that forces the negation of the winning condition regardless of the system's strategy.

### B.1 Proof for Theorem 2

In this section we prove:

**Theorem 2.** *Realizability and synthesis for weak Büchi games can be done in  $O(N)$  symbolic steps.*

**Algorithm 1** Weak Büchi winning memoryless strategy construction**Base Case.**  $\text{Win\_Aux}^0(X) := \text{Terminal}(X) \wedge \text{Acc}(X)$ , $\text{DC}^0(X) := \text{Terminal}(X)$ , and $\text{Fb\_Aux}^0(X, X') = \text{Terminal}(X) \wedge (\rho_{\mathcal{I}} \rightarrow \rho_{\mathcal{O}})(X)$ **Inductive Step.**

$$\text{DC}^{i+1}(X) := \forall X' : \text{Reach}(X, X') \rightarrow (\text{SCC}(X, X') \vee \text{DC}^i(X'))$$

$$\text{DC}_{\text{new}}^{i+1}(X) := \text{DC}^{i+1}(X) \setminus \text{DC}^i(X)$$

$$\text{N}^{i+1}(X) := \text{DC}_{\text{new}}^{i+1}(X) \wedge \neg \text{Acc}(X)$$

$$\text{A}^{i+1}(X) := \text{DC}_{\text{new}}^{i+1}(X) \wedge \text{Acc}(X)$$

$$\text{Win\_Aux}^{i+1}(X) := \text{Win\_Aux}^i(X)$$

$$\vee \text{Reachability}_{(\text{N}^{i+1}(X), \text{Win\_Aux}^i(X))}(X)$$

$$\vee \text{Safety}_{(\text{A}^{i+1}(X), \text{A}^{i+1}(X) \vee \text{Win\_Aux}^i(X))}(X)$$

$$\text{Fb\_Aux}^{i+1}(X, X') := \text{Fb\_Aux}^i(X, X')$$

$$\vee (\text{N}^{i+1}(X) \wedge \text{FReachability}_{(\text{N}^{i+1}(X), \text{Win\_Aux}^i(X))}(X, X'))$$

$$\vee (\text{A}^{i+1}(X) \wedge \text{FSafety}_{(\text{A}^{i+1}(X), \text{A}^{i+1}(X) \vee \text{Win\_Aux}^i(X))}(X, X'))$$

We remind that we denote the union  $\mathcal{I} \cup \mathcal{O}$  by  $X$ , and presented an  $O(N)$  time construction for the next BDDs (see Section 6.1, BDD Constructions):

$\text{SCC}(X, X')$ .  $(s, t') \models \text{SCC}(X, X')$  iff  $s$  and  $t$  belong to the same SCC of  $G$ , the game graph of the game structure  $GS$ .

$\text{Terminal}(X)$ .  $s \models \text{Terminal}(X)$  if  $s$  belongs to a terminal SCC  $S$ ; no other SCC is reachable from  $S$ .

To provide a rigorous proof for Theorem 2, in Algorithm 1 we modify the weak Büchi winning states construction from Section 6 to construct also a corresponding winning strategy. We remind some notations. Given sets of states  $A$  and  $B$ :

$\text{Reachability}_{(A,B)}(X)$ . A BDD for the states in  $A$  from which the system can force reaching  $B$ .

$\text{Safety}_{(A,B)}(X)$ . A BDD for the states in  $A$  from which the system can force the play to stay in  $B$ .

In addition to those BDDs, to reason about the weak Büchi strategy construction, we consider also their corresponding (memoryless) strategies:  $\text{FReachability}_{(A,B)}(X, X')$  and  $\text{FSafety}_{(A,B)}(X, X')$ . Note that these two strategies are given as BDDs over  $\mathcal{I} \cup \mathcal{O} \cup \mathcal{I}' \cup \mathcal{O}'$ , in compliance with the discussion given in Appendix A.

We argue that algorithm 1 is correct.

**Lemma 3.** *The fixed-points of  $\text{Win\_Aux}(X)$  and  $\text{Fb\_Aux}(X, X')$  in Algorithm 1 are BDDs for the winning states and a winning strategy in the weak Büchi game  $(GS, GF(\text{Acc}))$ , respectively.*

*Proof.* Let  $\text{Win}(X)$  and  $\text{Fb}(X, X')$  be the fixed-points of  $\text{Win\_Aux}(X)$  and  $\text{Fb\_Aux}(X, X')$ . We divide the proof into **soundness** and **completeness**. That is, we show that (a).  $\text{Fb}(X, X')$  wins from  $\text{Win}(X)$ , and (b). no other state is winning for the system.

**Soundness.** We show, by induction, that for each  $i$ ,  $\text{Fb\_Aux}^i(X, X')$  is a winning strategy from  $\text{Win\_Aux}^i(X)$ . The claim clearly holds for  $\text{Fb\_Aux}^0(X)$ , because every strategy is winning from the accepting terminal SCCs.

For the induction step, take  $s \in \text{Win\_Aux}^{i+1}(X)$ :

1. If  $s \in \text{Win\_Aux}^i(X)$  we are done by the induction hypothesis (note that  $\text{Fb\_Aux}^{i+1}(X, X')$  coincides with  $\text{Fb\_Aux}^i(X, X')$  on  $\text{Win\_Aux}^i(X)$ ).
2. If  $s \in \text{Reachability}_{(\mathbf{N}^{i+1}(X), \text{Win\_Aux}^i(X))}(X)$ ,  $\text{Fb\_Aux}^{i+1}(X, X')$  follows the next strategy from  $s$ : play reachability to reach  $\text{Win\_Aux}^i(X)$ , and then apply  $\text{Fb\_Aux}^i(X, X')$  for the rest of the play. By the induction hypothesis, any play consistent with this strategy is winning for the system.
3. Finally, if  $s \in \text{Safety}_{(\mathbf{A}^{i+1}(X), \mathbf{A}^{i+1}(X) \vee \text{Win\_Aux}^i(X))}(X)$ , the system plays the next strategy from  $s$ : play safety inside  $\mathbf{A}^{i+1}(X) \vee \text{Win\_Aux}^i(X)$ , and if the play traverses to  $\text{Win\_Aux}^i(X)$ , switch to  $\text{Fb\_Aux}^i(X, X')$ . Since all states of  $\mathbf{A}^{i+1}(X)$  are accepting, by the induction hypothesis, any play consistent with this strategy is winning for the system.

**Completeness.** We show, by induction, that for each  $i$ , the environment has a winning strategy from  $\text{DC}^i(X) \setminus \text{Win\_Aux}^i(X)$ . The claim clearly holds for  $i = 0$ , since every strategy for the environment is winning from the non-accepting terminal SCCs.

For the induction step, take  $s \notin \text{Win\_Aux}^{i+1}(X)$  (and thus  $s \notin \text{Win\_Aux}^i(X)$ ).

1. First, assume that  $s \in \mathbf{N}^{i+1}(X)$ .  
Since  $s \notin \text{Reachability}_{(\mathbf{N}^{i+1}(X), \text{Win\_Aux}^i(X))}(X)$ , the environment has a safety strategy on the region  $\mathbf{N}^{i+1}(X) \cup (\text{DC}^i(X) \setminus \text{Win\_Aux}^i(X))$  from  $s$ . A play consistent with this strategy either stays in  $\mathbf{N}^{i+1}(X)$ , or reaches  $\text{DC}^i(X) \setminus \text{Win\_Aux}^i(X)$ . By the induction hypothesis, in both cases the environment wins.
2. Otherwise,  $s \in \mathbf{A}^{i+1}(X)$ . Since  $s \notin \text{Safety}_{(\mathbf{A}^{i+1}(X), \mathbf{A}^{i+1}(X) \vee \text{Win\_Aux}^i(X))}(X)$ , the environment has a strategy to reach  $\text{DC}^i(X) \setminus \text{Win\_Aux}^i(X)$  from  $s$ . Hence, by the induction hypothesis, the environment has a winning strategy from  $s$ .  $\square$

To complete the proof of Theorem 2, we need to show that Algorithm 1 terminates in time  $O(N)$ .

**Lemma 4.** *For each  $i$ , the computation of  $\text{Reachability}_{(\mathbf{N}^{i+1}(X), \text{Win\_Aux}^i(X))}(X)$ ,  $\text{Safety}_{(\mathbf{A}^{i+1}(X), \mathbf{A}^{i+1}(X) \vee \text{Win\_Aux}^i(X))}(X)$ ,  $\text{FReachability}_{(\mathbf{N}^{i+1}(X), \text{Win\_Aux}^i(X))}(X, X')$ ,*

and  $\text{FSafety}_{(\mathbf{A}^{i+1}(X), \mathbf{A}^{i+1}(X) \vee \text{Win\_Aux}^i(X))}(X, X')$  is performed in  $O(|\text{DC}^{i+1}(X) \setminus \text{DC}^i(X)|)$  symbolic operations.

*Proof.* We start with  $\text{Reachability}_{(\mathbf{N}^{i+1}(X), \text{Win\_Aux}^i(X))}(X)$ . To compute this set of states we perform the next fixed-point computation in the sub-game over  $\text{DC}^{i+1}(X)$ :  $Z_0 = \text{Win\_Aux}^i(X)$ , and  $Z_{j+1} = \text{pre}_s(Z_j) \cup Z_j$ , where  $\text{pre}_s(Z)$  is the set of states from which the system can force reaching  $Z$  in a single step. Thus,  $Z_0 \subseteq Z_1 \subseteq \dots$ , and the winning region is  $Z_j$  that satisfies  $Z_j = Z_{j+1}$ . We refer the reader to [25, Chapter 20] for a comprehensive discussion.

Now, at each step  $j_0 < j$ , at least one state is added to  $Z_{j_0}$  thus there are at most  $|\text{DC}^{i+1}(X) \setminus \text{Win\_Aux}^i(X)|$  steps, each is performed in  $O(1)$  operations. Furthermore, if  $s \in \text{DC}^i(X) \setminus \text{Win\_Aux}^i(X)$ , then we never add  $s$  to a set  $Z_{j_0}$ . This claim is argued as follows. If we add  $s$  to some  $Z_{j_0}$ , then the system can force reaching  $\text{Win\_Aux}^i(X)$  from  $s$ , in contradiction to what we proved in Lemma 3 (specifically, the completeness). Hence, an upper bound of  $O(|\text{DC}^{i+1}(X) \setminus \text{DC}^i(X)|)$  operations is established.

A similar argument proves the same for  $\text{Safety}_{(\mathbf{A}^{i+1}(X), \mathbf{A}^{i+1}(X) \vee \text{Win\_Aux}^i(X))}(X)$ . This BDD is computed by  $Z_0 = \mathbf{A}^{i+1}(X) \vee \text{Win\_Aux}^i(X)$ , and  $Z_{j+1} = Z_j \cap \text{pre}_s(Z_i)$ . Thus,  $Z_0 \supseteq Z_1 \supseteq \dots$ , and the winning region is  $Z_j$  that satisfies  $Z_j = Z_{j+1}$ . As before, at each step  $j_0 < j$  at least a single state is removed from  $Z_{j_0}$  and hence, an upper bound of  $O(|\mathbf{A}^{i+1}(X) \vee \text{Win\_Aux}^i(X)|)$  steps holds. Furthermore, a state  $s \in \text{Win\_Aux}^i(X)$  is never removed from every  $Z_j$ . This claim is argued as follows. Take  $s \in \text{Win\_Aux}^i(X)$ , and assume that  $s \in Z_{j_0} \setminus Z_{j_0+1}$ . Consequently, the system cannot win the safety game from  $s$ . Hence, the environment has a strategy to reach  $\text{DC}^i(X) \setminus \text{Win\_Aux}^i(X)$  from  $s$ , in contradiction to what we have proved in Lemma 3. Therefore, the computation terminates after at most  $O(|\mathbf{A}^{i+1}(X)|) \leq O(|\text{DC}^{i+1}(X) \setminus \text{DC}^i(X)|)$  steps, as required.

Finally, by applying standard constructions, the strategies  $\text{FReachability}_{(\mathbf{N}^{i+1}(X), \text{Win\_Aux}^i(X))}(X, X')$  and  $\text{FSafety}_{(\mathbf{A}^{i+1}(X), \mathbf{A}^{i+1}(X) \vee \text{Win\_Aux}^i(X))}(X, X')$  are constructed in time  $O(|\text{DC}^{i+1}(X) \setminus \text{DC}^i(X)|)$  as well.  $\square$

We turn to prove Theorem 2.

*Proof (proof of Theorem 2).* By Lemma 3, Algorithm 1 computes both the system's winning region and a corresponding memoryless winning strategy. Lemma 4 implies that the algorithm terminates in time  $O(N)$ .

## B.2 Proofs for Theorem 3 and Theorem 4

In this section we prove:

**Theorem 3.** *Realizability for separated GR(k) games can be reduced to realizability of weak Büchi games.*

**Theorem 4.** *Let  $(GS, \varphi)$  be a separated GR(k) game over the input/output variables  $\mathcal{I}$  and  $\mathcal{O}$ . Then, the realizability and synthesis problems for  $(GS, \varphi)$  are solved in  $O(|\varphi| + N)$  and  $O(|\varphi|N)$  symbolic operations, respectively, where  $N = |2^{\mathcal{I} \cup \mathcal{O}}|$ .*

Consider a Separated GR( $k$ ) game  $(GS = (\mathcal{I}, \mathcal{O}, \theta_{\mathcal{I}}, \theta_{\mathcal{O}}, \rho_{\mathcal{I}}, \rho_{\mathcal{O}}), \varphi)$ , and write  $\varphi = \bigwedge_{l=1}^k \varphi_l$ , where  $\varphi_l = \bigwedge_{i=1}^{n_l} \text{GF}(a_{l,i}) \rightarrow \bigwedge_{j=1}^{m_l} \text{GF}(g_{l,j})$ . Let  $\text{acc}$  be the assertion expressing the set of accepting states, as depicted in Section 5.1: For a state  $s$  in an SCC  $S$ , with projections  $S_{\mathcal{I}}$  on  $G_{\mathcal{I}}$  and  $S_{\mathcal{O}}$  on  $G_{\mathcal{O}}$ ,  $s$  is accepting if for *every* constraint  $\varphi_l$ , where  $l \in \{1, \dots, k\}$ , one of the following holds:

**All guarantees hold in  $S$ .** For every  $j \in \{1, \dots, m_l\}$ , there exists  $o \in S_{\mathcal{O}}$  such that  $o \models g_{l,j}$ .

**Some assumption cannot hold in  $S$ .** There exists  $j \in \{1, \dots, n_l\}$  such that for all  $i \in S_{\mathcal{I}}$ ,  $i \not\models a_{l,j}$ .

**Lemma 5.** *A BDD  $\text{Acc}(X)$  such that  $s \models \text{Acc}(X)$  iff  $s$  is accepting, can be constructed in  $O(|\varphi| + N)$  symbolic operations.*

*Proof.* Consider the BDD  $\text{SCC}(X, X')$ , constructed in  $O(N)$  operations (see Section B.1), and take a component  $\varphi_l = \bigwedge_{i=1}^{n_l} \text{GF}(a_{l,i}) \rightarrow \bigwedge_{j=1}^{m_l} \text{GF}(g_{l,j})$ . First, we identify all states that their SCC includes a  $g_{l,j}$ -state. For  $j \in \{1, \dots, m_l\}$ , let  $\text{GAR}_{l,j}(X, X')$  be a BDD such that  $(i_0, o_0, i'_1, o'_1) \models \text{GAR}_{l,j}(X, X')$  iff  $o_1 \models g_{l,j}$ . Write  $\text{SGAR}_{l,j}(X) := \exists X'(\text{SCC} \wedge \text{GAR}_{l,j})$ . Therefore,  $s \models \text{SGAR}_{l,j}(X)$  iff the SCC of  $s$  includes a  $g_{l,j}$ -state.

Now, we focus on the assumptions. In similar to the former case, let  $\text{ASM}_{l,j}(X, X')$  be a BDD such that  $(i_0, o_0, i'_1, o'_1) \models \text{ASM}_{l,j}$  iff  $i_1 \models a_{l,i}$ . Write  $\text{SASM}_{l,j}(X) := \forall X'(\text{SCC}(X, X') \rightarrow \neg \text{ASM}_{l,j}(X, X'))$ . Therefore,  $s \models \text{SASM}_{l,j}(X)$  iff  $s$ 's SCC does not include an  $a_{l,i}$ -state.

As a result, the BDD  $\text{Acc} := \bigwedge_{l=1}^k ((\bigwedge_{j=1}^{m_l} \text{SGAR}_{l,j}) \vee (\bigvee_{i=1}^{n_l} \text{SASM}_{l,i}))$  satisfies the require, and its construction is performed in time  $O(|\varphi| + N)$ .  $\square$

After constructing the BDD  $\text{Acc}(X)$  for  $\text{acc}$ , we can obtain a winning strategy  $f_B$  for the weak Büchi game  $(GS, \text{GF}(\text{acc}))$  via Algorithm 1. Algorithm 2 then describes how to construct a winning strategy  $f$  for the separated GR( $k$ ) game  $(GS, \varphi)$  using  $\text{acc}$ ,  $f_B$  and the strategy  $f_{\text{travel}}$  for visiting all guarantees in an SCC.

The strategy  $f_{\text{travel}}$  is described in Section 6.2 and detailed in the second part of Algorithm 2. Note that, for the sake of presentation, we assume that if  $s \in S$ , an SCC that includes no  $gar_j$ -state, then the reachability strategy  $f_{r(j)}(s, i)$  for guarantee  $gar_j$  returns a distinguished value  $\perp$ . If all  $f_{r(j)}$  return  $\perp$ , then no guarantee is satisfiable in  $S$ , and therefore  $f_{\text{travel}}$  simply returns an arbitrary output that remains inside  $S$  (line 17). Also note that  $f_{\text{travel}}$  updates its memory output variable  $\text{mem}$  whenever it reaches a state that satisfies a guarantee (line 12), and  $f$  resets  $\text{mem}$  whenever it switches from  $f_{\text{travel}}$  to  $f_B$  (line 4).

**Lemma 6.** *Let  $W$  be the system's winning region for the weak Büchi game  $B = (GS, \text{GF}(\text{acc}))$ . Then, Algorithm 2 constructs a winning strategy from  $W$ .*

*Proof.* We will prove that if  $s \in W$ , then the strategy  $f$  described in Algorithm 2 wins  $(GS, \varphi)$  from  $s$ . We reason by cases.

First, consider the case where  $s \models \text{acc}$ , i.e.,  $s$  is in an accepting SCC  $S$ . Then,  $f(s, i)$  returns the output of  $f_{\text{travel}}(s, i)$ . There are two possibilities:

**Algorithm 2** A separated  $\text{GR}(k)$  Winning Strategy

---

```

/*      Implementation of  $f(s, i)$       */
1: if  $s \models acc$  then
2:   return  $f_{travel}(s, i)$ 
3: else
4:    $mem = 0$ 
5:   return  $f_B(s, i)$ 
6: end if

/*      Implementation of  $f_{travel}(s, i)$       */
7: for  $i = 0$  to  $m - 1$  do
8:    $next\_gar = mem + i \bmod m$ 
9:    $o = f_{r(next\_gar)}(s, i)$ 
10:  if  $o \neq \perp$  then
11:    if  $(i, o) \models gar_{next\_gar}$  then
12:       $mem = next\_gar + 1$ 
13:    end if
14:    return  $o$ 
15:  end if
16: end for
17: return  $o$  in the same SCC  $S_O$  of  $s|_O$ 

```

---

- $f_{travel}$  returns from line 17. This is only possible if  $f_{r(next\_gar)}(s, i) = \perp$  for every  $next\_gar \in \{0, \dots, m - 1\}$ , meaning that there is no state in  $S$  that satisfies any of the guarantees  $gar_{next\_gar}$ . But by definition of accepting SCCs, this means that there must be no  $\varphi_l$  for which all assumptions can be satisfied from inside  $S$ . Therefore, as long as the play remains inside  $S$ ,  $\varphi$  is vacuously satisfied and the system wins. Note that in this case,  $f_{travel}$  will always return from line 17, and therefore always remain in  $S$  unless the environment chooses an input that takes the play to a different SCC. In that case, however, by Theorem 1 the new SCC will also be inside the winning region.
- $f_{travel}$  returns from line 14, and therefore returns the output from some function  $f_{r(next\_gar)}$ . By construction of  $f_{r(next\_gar)}$ , the output remains inside the same SCC and makes progress toward reaching a state that satisfies  $gar_{next\_gar}$ . Note that the same  $f_{r(next\_gar)}$  will be chosen next time until  $gar_{next\_gar}$  is reached, at which point  $mem$  will be updated to  $next\_gar + 1 \bmod m$ . Therefore, as long as the play remains inside  $S$ ,  $f_{travel}$  will cycle through all  $gar_{next\_gar}$  that can be satisfied from  $S$ . This means that every  $\varphi_l$  such that all guarantees hold in  $S$  will be satisfied. Since  $S$  is an accepting SCC, the only remaining  $\varphi_l$ s are those where some assumption cannot hold in  $S$ , which will therefore be vacuously satisfied. Therefore, the system is guaranteed to win while it remains in  $S$ . If the environment chooses an input that takes the play to a different SCC, again by Theorem 1 the new SCC will also be inside the winning region.



Next, consider the case where  $s \not\models acc$ , i.e.,  $s$  is in a non-accepting SCC. In this case,  $f(s, i)$  sets  $mem$  to 0 and returns the output of  $f_B(s, i)$ . Since  $s \in W$  and  $f_B$  is a winning strategy for  $B$ ,  $f_B(s, i)$  is guaranteed to remain in  $W$  and move towards an accepting SCC, as this is the only way for the system to win  $B$ . Since  $f(s, i)$  will keep returning  $f_B(s, i)$  while in a non-accepting SCC, the play is guaranteed to eventually reach an accepting SCC  $S$ . At this point  $f$  will switch back to  $f_{travel}$ .

Therefore,  $f$  is guaranteed to always satisfy the winning condition  $\varphi$  while the play remains inside an accepting SCC (via  $f_{travel}$ ), and it is guaranteed to always reach an accepting SCC from a non-accepting SCC (via  $f_B$ ). Since the set of SCCs is finite and partially ordered by reachability, every play is guaranteed to eventually stay forever in a single SCC  $S$ . Then, the two conditions above guarantee that  $S$  will be accepting and that  $f$  will win from  $S$ .  $\square$

**Lemma 7.** *Let  $W$  be the system's winning region for the weak Büchi game  $B = (GS, GF(acc))$ . Then, if  $s \notin W$ , the system cannot win the separated  $GR(k)$  game  $(GS, \varphi)$  from  $s$ .*

*Proof.* Since  $s \notin W$ , there is no strategy that allows the system to force the play to converge to an accepting SCC. Since every play must converge to some SCC, the environment can force the play to converge to a non-accepting SCC from  $s$ .

Note that an SCC  $S$  is non-accepting if there is at least one  $\varphi_l$  that the system cannot satisfy from inside  $S$ . That is, the environment can visit all the assumptions but the system cannot visit all the guarantees in  $S$ .

Therefore, we can construct a function  $f_{travel}^e$  for the environment that is analogous to the function  $f_{travel}$  for the system but cycles through all assumptions rather than all guarantees. Note that  $f_{travel}^e$  is guaranteed to win for the environment as long as the play remains inside a non-accepting SCC.

Finally, note that a Delay Property analogous to Theorem 1 can be proved for the environment by simply swapping inputs and outputs. Therefore, the environment can ensure that the play always remains outside of  $W$ , it converges to a non-accepting SCC, and the environment can win from that SCC (via  $f_{travel}^e$ ). Therefore, the system cannot win the separated  $GR(k)$  game from  $s$ .  $\square$

Clearly, Theorem 3 immediately follows from Lemmas 6 and 7. For Theorem 4, the complexity of realizability follows from Lemmas 5, 6 and 7 and Theorem 2. The complexity of synthesis follows from realizability with the addition of the computation of  $f_{travel}$ , which requires computing a reachability game for each  $f_{r(j)}$ , taking  $O((\#gars)N) \leq O(|\varphi|N)$  symbolic operations.