2016 IEEE 55th Conference on Decision and Control (CDC)
ARIA Resort & Casino
December 12-14, 2016, Las Vegas, USA

Symbolic Synthesis with Average Performance Guarantees

Matthias Rungger, Gunther Reissig, and Majid Zamani

Abstract— **We consider a general quantitative controller synthesis framework to synthesize controllers that not only enforce a desired input-output behavior on the closed-loop, but additionally minimize a certain average cost function, which is used to assess the closed loop behavior. We follow the usual symbolic synthesis approach, based on so-called discrete abstractions (also known as symbolic models) and propose a modification of the well-known system relations which enables the reasoning about the closed loop performance across related systems. We show how to construct symbolic models in terms of the newly introduced system relations for sampled-data, switched, nonlinear systems. A small numerical example is provided, to illustrate some of the theoretical results.**

I. INTRODUCTION

Quantitative objectives have been considered in the control systems community from the very beginning of the analysis of controller design problems [1, 2]. Value functions that arise in the context of infinite-horizon optimal control problems, are often also Lyapunov functions. Therefore, quantitative objectives naturally appear in connection with (robust) stabilization problems [3]. The situation is different for the classical synthesis methods of reactive systems [4–7]. Here the objective is of qualitative nature, i.e., the synthesized system either conforms to the specification, or violates it.

In the recent years, there has been a considerable effort from the control systems community [8–14] as well as from the reactive systems community [15–20], to combine the classical approaches from the different fields and provide synthesis methods that are able to simultaneously account for complex specifications, e.g., formulated in linear temporal logic (LTL) [7], and quantitative objectives, e.g., average costs [21] (also known as mean-payoff objectives [22, 23]).

In this work, we follow this trend and consider controller synthesis problems, in which the specification is given as a set of desired input-output signals and a cost function, which assesses the worst-case average costs associated with the close loop behavior. The objective is to find a controller that simultaneously enforces the desired input-output signals on the plant and minimizes the given cost function. Similar synthesis problems with average costs have been analyzed in [8, 13, 15, 20]. This line of research concentrates on the development of novel algorithms, which are applicable to the quantitative synthesis problems, and to establish the computational complexity of the proposed algorithms. In this paper, we extend those approaches (which are limited to finite systems) to infinite systems via the usual abstraction and refinement principle, which is well-known in the context of traditional, qualitative language-containment specifications [24, 25]. In this framework, a so-called *abstraction* also known as *symbolic model*, i.e., a finite system, is used as a substitute in the controller design process. The correctness of this framework is usually ensured by showing that the behavior of the abstract closed loop majorizes (up to a certain accuracy) the behavior of the concrete closed loop. On a technical level, such statements are achieved by relating the *plant*, i.e., the given infinite concrete system, with the abstraction via certain system relations, e.g. (approximate) bisimulation relations [10], alternating simulation relations [24] or feedback refinement relations [25].

In this work, similar to [26], we use *valuated alternating simulation relations* and *valuated feedback refinement relations*, i.e., variants of the well-known system relations for controller refinement [24, 25], as a means to establish the majorization of the concrete closed loop by the abstract closed loop not only in terms of behavioral inclusion, but also in terms of the cost functions associated with the respective controllers. Additionally, we show that the existence of a valuated system relation from one system to another one, implies that the value function, i.e., the best achievable performance, associated with the first system is bounded by the value function associated with the second system. After the presentation of the general theory, we focus on sampled-data, switched, nonlinear systems and "reach and stay while avoid" specifications under average costs. We provide two algorithms to construct, finite auxiliary synthesis problems, whose solutions provide upper and lower bounds on the value function of the concrete control problem. The upper bounding control problem, whose construction is adapted from [25], is simultaneously used to derive a controller for the plant to enforce the given reach and stay while avoid specification.

Abstraction and refinement procedures to solve quantitative synthesis problems have previously been proposed in [9–12, 27]. In [9–12] reachability specifications in combination with cost functions to evaluate the transient behavior of the system are considered. In [27], synthesis algorithms to enforce safety specifications in combination with a receding horizon optimization scheme have been developed. In contrast to those approaches, we consider general specifications and long-term, infinite-horizon, average costs. Here

M. Rungger and M. Zamani are with the Department of Electrical and Computer Engineering at the Technical University of Munich, 80333 Munich, Germany, matthias.rungger@tum.de, zamani@tum.de, http://www.hcs.ei.tum.de.

G. Reissig is with the University of the Federal Armed Forces Munich, Dept. Aerospace Eng., Chair of Control Eng. (LRT-15), D-85577 Neubiberg (Munich), Germany, gunther@reiszig.de, http://www.reiszig.de/gunther.

This work was supported in part by the German Research Foundation (DFG) through the grant ZA 873/1-1 and the TUM International Graduate School of Science and Engineering (IGSSE).

978-1-5090-1837-6/16/$31.00 ©2016 IEEE

the long-term performance is the most crucial performance measure and the transient behavior is of minor importance. Our approach is particularly appealing in the context of switched systems to enforce reach and stay specification while minimizing the average number of switches.

II. Notation

$\mathbb{R}$, $\mathbb{R}_+$, $\mathbb{Z}$ and $\mathbb{Z}_+$ denote the sets of real numbers, non-negative real numbers, integers and non-negative integers, respectively, and $\mathbb{N} = \mathbb{Z}_+ \setminus \{0\}$. We adopt the convention that $\pm\infty + x = \pm\infty$ for any $x \in \mathbb{R}$ and $\inf \varnothing = \infty$. We denote by $[a, b]$, $]a, b[$, $[a, b[$, and $]a, b]$ closed, open and half-open, respectively, intervals with end points a and b. The notations $[a; b]$, $]a; b[$, $[a; b[$, and $]a; b]$ stand for discrete intervals, e.g. $[a; b] = [a, b] \cap \mathbb{Z}$, $[1; 4[= \{1, 2, 3\}$, and $[0; 0[= \varnothing$. For $a, b \in (\mathbb{R} \cup \{\infty, -\infty\})^n$, the closed hyper-interval $[\![a, b]\!]$ is defined by $[\![a, b]\!] = \mathbb{R}^n \cap ([a_1, b_1] \times \cdots \times [a_n, b_n])$. In $\mathbb{R}^n$, the relations $<, \leq, \geq, >$ are defined component-wise, i.e., $a < b$ iff $a_i < b_i$ for all $i \in [1; n]$. Similarly, for $x \in \mathbb{R}^n$ we use $|x| \in \mathbb{R}^n_+$ to denote the component-wise norm of x, i.e., the ith component of $|x|$ is given by the absolute value of x_i.

We denote by $f\colon A \rightrightarrows B$ a *set-valued map* of A into B, whereas $f\colon A \to B$ denotes an ordinary map; see [28]. If f is set-valued, then f is *strict* and *single-valued* if $f(a) \neq \varnothing$ and $f(a)$ is a singleton, respectively, for every a. Throughout the text, we denote the identity map $X \to X\colon x \mapsto x$ by id. The domain of definition X will always be clear from the context.

We identify set-valued maps $f\colon A \rightrightarrows B$ with binary relations on $A \times B$, i.e., $(a, b) \in f$ iff $b \in f(a)$. We denote by $f \circ g$ the composition of f and g, $(f \circ g)(x) = f(g(x))$. Moreover, if f is single-valued, it is identified with an ordinary map $f\colon A \to B$. The set of maps $A \to B$ is denoted by B^A, and the set of all signals $\beta : [0; T[\to B$ is denoted by $B^{[0;T[}$. We set $B^\infty := \bigcup_{T \in \mathbb{Z}_+ \cup \{\infty\}} B^{[0;T[}$ and for $\beta \in B^\infty$, use $\operatorname{dom} \beta$ to denote the interval on which β is defined.

III. Control Problems with Average Costs

In this work we consider *plants*, which are given as discrete-time, non-deterministic systems of the form

$$\xi(t + 1) \in F(\xi(t), \alpha(t)) \tag{1}$$

where $\xi(t) \in X$ and $\alpha(t) \in A$ are the state, respectively, input signals and $F : X \times A \rightrightarrows X$ is the transition function. The plant is a particular instance of a more general notation of system [25] that provides a unified definition for plants, controllers and quantizers.

Definition 1. *A* system *is a septuple*

$$S = (X, X_0, A, B, Z, F, H), \tag{2}$$

where X, X_0, A, B and Z denote the state*,* initial state*,* input*,* internal input *and* output alphabet*, respectively. The sets X, X_0, A, B and Z are assumed to be nonempty, $X_0 \subseteq X$, $H\colon X \times A \rightrightarrows Z \times B$ is strict, and $F\colon X \times B \rightrightarrows X$. A quadruple $(\alpha, \beta, \xi, \zeta) \in A^{[0;T[} \times B^{[0;T[} \times X^{[0;T[} \times Z^{[0;T[}$ is a* solution *of the system* (2) *(on $[0; T[$, starting at $\xi(0)$) if $T \in \mathbb{Z}_+ \cup \{\infty\}$, $\xi(0) \in X_0$ and*

$$\forall_{t \in [0; T-1[} : \quad \xi(t + 1) \in F(\xi(t), \beta(t))$$
$$\forall_{t \in [0; T[} : \quad (\zeta(t), \beta(t)) \in H(\xi(t), \alpha(t)).$$

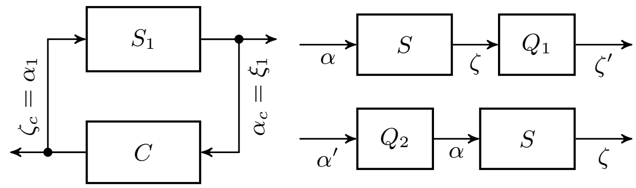

Fig. 1. Left: feedback composed system $C \times S_1$. Right: Serial composed systems $Q_1 \circ S$ and $S \circ Q_2$.

A system is basically a Mealy-type transition system with non-deterministic output and transition functions, see [25] for more details.

Given a system $S_1 = (X_1, X_{1,0}, A_1, B_1, Z_1, F_1, H_1)$ that satisfies $X_{1,0} = X_1 = Z_1$, $A_1 = B_1$ and $H_1 = \mathrm{id}$, we recover the notion of the plant in (1). Such a system is termed a *simple system* and denoted by $S_1 = (X_1, A_1, F_1)$.

Definition 2. *A system $C = (X_c, X_{c,0}, A_c, B_c, Z_c, F_c, H_c)$ is a* controller *for $S_1 = (X_1, A_1, F_1)$ if it satisfies*

$$Z_c \subseteq A_1 \wedge X_1 \subseteq A_c \text{ and}$$
$$(a_1, b_c) \in H_c(x_c, x_1) \wedge F_1(x_1, a_1) = \varnothing \Rightarrow F_c(x_c, b_c) = \varnothing.$$

The first condition ensures that the inputs and outputs of the controller and the plant are compatible in a feedback composition. The second condition is required in the controller transfer across related systems, see [25].

The *closed loop* $C \times S_1$, resulting from the feedback composition of a controller C and a simple system S_1 is a system that is obtained by connecting the output ζ_c of C with the input α_1 of S_1 and vice versa, see Fig. 1 and [25, Def. III.3].

Definition 3. *The* behavior *$\mathcal{B}(C \times S_1)$ is the set of input-output sequences $(\alpha_1, \xi_1) \in (A_1 \times X_1)^{[0;T[}$, $[0; T[\subseteq \mathbb{Z}_+$ for which there exist signals (β_c, ξ_c) so that $(\alpha_1, \alpha_1, \xi_1, \xi_1)$ and $(\xi_1, \beta_c, \xi_c, \alpha_1)$ are a solution of S and C, respectively. In case that $T \in \mathbb{Z}_+$, then $F_1(\xi_1(T-1), \alpha_1(T-1)) = \varnothing$ or $F_c(\xi_c(T-1), \beta_c(T-1)) = \varnothing$ must hold. The behavior associated with a particular state $x \in X_1$ is given by*

$$\mathcal{B}_x(C \times S_1) = \{(\alpha, \xi) \in \mathcal{B}_x(C \times S_1) \mid \xi(0) = x\}.$$

A *specification* for $S_1 = (X_1, A_1, F_1)$ is simply given as a set $\Sigma_1 \subseteq (A_1 \times X_1)^\infty$ with which we describe the desired closed loop behavior. The system S_1 together with specification Σ_1 constitute a *control problem* (S_1, Σ_1). We say that a system C *solves the control problem* (S_1, Σ_1) if C is a controller for S_1 and the following inclusion holds

$$\mathcal{B}(C \times S_1) \subseteq \Sigma_1.$$

The set of all controllers C that solve a control problem (S_1, Σ_1) is denoted by $\mathcal{C}(S_1, \Sigma_1)$.

Additionally to the requirement that a controller C solves the control problem (S_1, Σ_1) we would like that C minimizes a certain average cost function. To this end, we assume we are given a *running cost function* for $S_1 = (X_1, A_1, F_1)$ by

$$G_1 : (A_1 \times X_1)^2 \to \mathbb{R} \cup \{\pm\infty\}$$

and consider the *cost function* $J_1 : X_1 \to \mathbb{R} \cup \{\pm\infty\}$ associated with a controller $C \in \mathcal{C}(S_1, \Sigma_1)$ defined by

$$J_1(x) = \infty \tag{3a}$$

if there exists $(\alpha, \xi) \in \mathcal{B}_x(C \times S_1)$ with $\mathrm{dom}(\alpha, \xi) \neq [0; \infty[$ and otherwise by

$$J_1(x) = \sup_{(\alpha,\xi)\in\mathcal{B}_x(C\times S_1)} \limsup_{t\to\infty} \frac{1}{t+1} L_1(t, \alpha, \xi) \tag{4a}$$

with $L_1 : \mathbb{Z}_+ \times (A_1 \times X_1)^{[0;\infty[} \to \mathbb{R} \cup \{\pm\infty\}$ given by

$$L_1(t, \alpha, \xi) = \sum_{t'=0}^{t} G_1(\alpha(t'), \xi(t'), \alpha(t'+1), \xi(t'+1)). \tag{5}$$

The best achievable performance is given by the *value function* $V_1 : X_1 \to \mathbb{R} \cup \{\pm\infty\}$ associated with (S_1, G_1, Σ_1) by

$$V_1(x) = \inf_{C\in\mathcal{C}(S_1,\Sigma_1)} J_1(x). \tag{6}$$

Definition 4. *A control problem (S_1, Σ_1) together with a running cost function G_1 for S_1 constitute a* valuated control problem *(S_1, G_1, Σ_1).*

It is well-known that even if the plant is *finite*, i.e., the input and state alphabet of the plant are finite sets, depending on the particular specification, the optimal controller potentially requires infinite memory, see e.g. [20]. However, for the particularly appealing class of reach and stay specifications, which we envision in this work and which are often used in the context of asymptotic stabilization of a control systems around a desired set point [29], it is known that *memoryless* or *static* optimal controller exist, i.e., the controller state alphabet is a singelton, see [15, Thm. 5].

Before we conclude this section, we shortly define the *serial composition* of a strict map $Q_1 : Z \rightrightarrows Z'$ and a system S of the form (2), as a system $Q_1 \circ S$ which is given by $(X, X_0, A, B, Z', F, H')$ with the output function $H'(x, a) = \{(z', b') \mid \exists_{(z,b)\in H(x,a)} z' \in Q_1(z) \wedge b = b'\}$. Similarly, given a strict map $Q_2 : A' \rightrightarrows A$, we use $S \circ Q_2$ to denote the system $(X, X_0, A', B, Z, F, H')$ with the output function $H'(x, a') = H(x, Q_2(a'))$ for all $x \in X$, $a' \in A'$. Both compositions are illustrated in Fig. 1.

IV. Valuated System Relations

We introduce valuated system relations as a means to relate the cost functions and the value functions across related systems. We consider alternating simulation relations [24] as well as feedback refinement relations [25], in order to facilitate the performance comparison with respect to average, infinite-horizon cost criteria. In [26], we introduced valuated system relations in the context of optimal stopping problems.

Subsequently, we need a notion of admissible inputs. Given a simple system $S = (X, A, F)$, we define the set of *admissible inputs at the state $x \in X$* by

$$A_S(x) = \{a \in A \mid F(x, a) \neq \varnothing\}.$$

Definition 5. *Consider two simple systems with running cost functions*

$$S_i = (X_i, A_i, F_i), \qquad i \in \{1, 2\},$$
$$G_i : (A_i \times X_i)^2 \to \mathbb{R}.$$

A relation $R_e \subseteq X_1 \times X_2 \times A_1 \times A_2$ whose projection onto $X_1 \times X_2$, i.e., $R := \{(x_1, x_2) \mid \exists_{a_i\in A_i} : (x_1, x_2, a_1, a_2) \in R_e\}$ is strict, is a valuated alternating simulation relation *from*[1] *(S_1, G_1) to (S_2, G_2), if*

$$\begin{aligned} &\forall_{(x_1,x_2)\in R} \forall_{a_2\in A_2} \exists_{a_1\in A_1} : (x_1, x_2, a_1, a_2) \in R_e \\ &\forall_{(x_1,x_2,a_1,a_2)\in R_e} : a_2 \in A_{S_2}(x_2) \implies a_1 \in A_{S_1}(x_1) \end{aligned} \tag{7a}$$

$$\forall_{(x_1,x_2,a_1,a_2)\in R_e} \forall_{x_1'\in F_1(x_1,a_1)} \exists_{x_2'\in F_2(x_2,a_2)} : (x_1', x_2') \in R \tag{7b}$$

$$\begin{aligned} &\forall_{(x_1,x_2,a_1,a_2),(x_1',x_2',a_1',a_2')\in R_e} \\ &\qquad G_1(a_1, x_1, a_1', x_1') \leq G_2(a_2, x_2, a_2', x_2'). \end{aligned} \tag{7c}$$

A valuated alternating simulation relation R_e from (S_1, G_1) to (S_2, G_2) is called valuated feedback refinement relation *from (S_1, G_1) to (S_2, G_2) if $A_2 \subseteq A_1$ and*

$$(x_1, x_2, a_1, a_2) \in R_e \implies a_1 = a_2 \tag{8a}$$
$$(x_1, x_2, a_1, a_2) \in R_e \implies R(F_1(x_1, a_1)) \subseteq F_2(x_2, a_2) \tag{8b}$$

The requirements (7a) and (7b) are the usual conditions for alternating simulation relations [24, Def. 4.19], while (7c) is new. Note that the main objective of those system relations is to enable the controller transfer also known as *controller refinement* from system S_2 to the system S_1. In this context, S_2 assumes the role of the abstraction, while S_1 corresponds to the plant. Consider two related states $(x_1, x_2) \in R$ and suppose on the abstract closed loop an admissible input $a_2 \in A_2(x_2)$ is applied to S_2. Then (7a) ensures that there exist an admissible input $a_1 \in A_1(x_1)$ (in the relation R_e) that can be applied to S_1. Subsequently, (7b) guarantees that any successor $x_1' \in F_1(x_1, a_1)$ can be matched by a successor $x_2' \in F_2(x_2, a_2)$ so that the successor states are related $(x_1', x_2') \in R$ and the process can be repeated. With (7c) in place, it is guaranteed that the running costs G_1 are upper bounded by G_2.

Feedback refinement relations have been introduced in [25] to address certain shortcomings of the controller refinement mechanism based on alternating simulation relations, see [25, Sec. IV]. Specifically, feedback refinement relations enable a straightforward controller refinement, i.e., given a controller C for an abstraction S_2, the controller for the plant S_1 is simply given by $C \circ R$, see [25, Thm. VI.3].

[1]With this definition we follow the notions in [25, 30] as apposed to [24, Def. 4.19] in which the conditions (7a) and (7b) correspond to an alternating simulation relation from S_2 to S_1.

We extend the notion of alternating simulation relations to valuated control problems.

Definition 6. *Consider two valuated control problems* $i \in \{1,2\}$, (S_i, G_i, Σ_i) *with* $S_i = (X_i, A_i, F_i)$. *A valuated alternating simulation relation* R_e *from* (S_1, G_1) *to* (S_2, G_2) *is called a* valuated alternating simulation relation from (S_1, G_1, Σ_1) to (S_2, G_2, Σ_2) *if for all* $T \in \mathbb{Z}_+ \cup \{\infty\}$

$$(\xi_1, \xi_2, \alpha_1, \alpha_2) \in R_e^{[0;T[} \wedge (\alpha_2, \xi_2) \in \Sigma_2 \implies (\alpha_1, \xi_1) \in \Sigma_1. \tag{9}$$

The fact that R_e and Q_e are valuated alternating simulation, respectively, valuated feedback refinement relation from (S_1, G_1, Σ_1) to (S_2, G_2, Σ_2) is denoted by

$$(S_1, G_1, \Sigma_1) \preceq_{R_e} (S_2, G_2, \Sigma_2)$$
$$(S_1, G_1, \Sigma_1) \preccurlyeq_{Q_e} (S_2, G_2, \Sigma_2).$$

Valuated system relations enable the following theorem.

Theorem 1. *Let* (S_i, G_i, Σ_i), $i \in \{1,2\}$ *be two valuated control problems and let* R_e *be a valuated alternating simulation relation from* (S_1, G_1, Σ_1) *to* (S_2, G_2, Σ_2). *If* C_2 *solves* (S_2, Σ_2) *then there exists a controller* C_1 *that solves* (S_1, Σ_1) *and the cost functions* J_i *associated with* $C_i \in \mathcal{C}(S_i, \Sigma_i)$ *satisfy*

$$\forall_{x_1 \in X_1} \exists_{x_2 \in R(x_1)} : J_1(x_1) \leq J_2(x_2). \tag{10}$$

If R_e *is a valuated feedback refinement relation form* (S_1, Σ_1) *to* (S_2, Σ_2) *then* $C_1 = C_2 \circ R$.

Theorem is based on the following lemma.

Lemma 1. *Consider the context of Theorem 1 and let* $S_i = (X_i, A_i, F_i)$. *If* C_2 *is a controller for* S_2, *then there exists a controller* C_1 *for* S_1 *so that for any* $(\alpha_1, \xi_1) \in \mathcal{B}(C_1 \times S_1)$ *defined on* $[0;T[\subseteq \mathbb{Z}_+$, *there exists* $(\alpha_2, \xi_2) \in \mathcal{B}(C_2 \times S_2)$ *defined on* $[0;T[$ *so that* $(\xi_1, \xi_2, \alpha_1, \alpha_2) \in R_e^{[0;T[}$.
If R_e *is a valuated feedback refinement relation form* (S_1, Σ_1) *to* (S_2, Σ_2) *then* $C_1 = C_2 \circ R$.

Subsequently, we term the controller C_1 that is referred to in Lemma 1 as the *refined controller from* C_2, S_2, S_1 and R_e.

For feedback refinement relations, Lemma 1 follows directly from [25, Thm. V.4(iii)]. For alternating simulations relations the lemma is close to [24, Prop. 8.7].

Theorem 2. *Let* (S_i, G_i, Σ_i), $i \in \{1,2\}$ *be two valuated control problems and* V_i *be the associated value functions* (6). *Suppose there exists a relation* R_e *so that* $(S_1, G_1, \Sigma_1) \preceq_{R_e} (S_2, G_2, \Sigma_2)$. *Then*

$$\forall_{(x_1, x_2) \in R} : \quad V_1(x_1) \leq V_2(x_2). \tag{11}$$

Theorem 2 utilizes the following lemma.

Lemma 2. *Consider the context of Theorem 2. Let* C_2 *solve* (S_2, Σ_2) *and fix* $(x_1, x_2) \in R$. *There exists a controller* C_1 *that solves* (S_1, Σ_1) *and for any* $(\alpha_1, \xi_1) \in \mathcal{B}_{x_1}(C_1 \times S_1)$ *defined on* $[0;T[\subseteq \mathbb{Z}_+$, *there exists* $(\alpha_2, \xi_2) \in \mathcal{B}_{x_2}(C_2 \times S_2)$ *defined on* $[0;T[$ *so that* $(\xi_1, \xi_2, \alpha_1, \alpha_2) \in R_e^{[0;T[}$.

In the next section, we analyze valuated control problems (S_1, G_1, Σ_1) for sampled-data switched systems and reach and stay while avoid specifications. We show how to construct two auxiliary valuated control problems $(\hat{S}_2, \hat{G}_2, \hat{\Sigma}_2)$ and $(\check{S}_2, \check{G}_2, \check{\Sigma}_2)$ so that there exist relations Q_e and R_e such that

$$(\check{S}_2, \check{G}_2, \check{\Sigma}_2) \preceq_{R_e} (S_1, G_1, \Sigma_1) \preccurlyeq_{Q_e} (\hat{S}_2, \hat{G}_2, \hat{\Sigma}_2).$$

From Theorem 2 we obtain the inequalities

$$\forall_{x_1 \in X_1} \forall_{\check{x}_2 \in R^{-1}(x_1)} \forall_{x_2 \in Q(x_1)} : \quad \check{V}_2(\check{x}_2) \leq V_1(x_1) \leq \hat{V}_2(\hat{x}_2).$$

Moreover, by solving the control problem $(\hat{S}_2, \hat{G}_2, \hat{\Sigma}_2)$ we obtain a controller C that we refine to $C \circ Q$, which solves (S_1, G_1, Σ_1). An upper bound on the performance (cost function) of $C \circ Q$ follows from Theorem 1 by

$$J_1(x_1) \leq \sup_{x_2 \in Q(x_1)} J_2(x_2).$$

V. Application to Switched Systems

A. The Valuated Control Problem

We consider switched non-linear systems given by differential equations of the form

$$\dot{\xi}(t) = f(\xi(t), u) \tag{12}$$

where $f : \mathbb{R}^n \times U \to \mathbb{R}^n$ and $U \subseteq \mathbb{R}^m$. We assume that U is non-empty, *finite* and that $f(\cdot, u)$ is continuously differentiable for all $u \in U$. We use φ to denote the general solution of (12) for constant inputs, i.e., if $x \in \mathbb{R}^n$, $u \in U$, then $\varphi(\cdot, x, u)$ is the unique non-continuable solution of the initial value problem $\dot{\xi} = f(\xi, u)$, $\xi(0) = x$ [31].

We are interested in designing controllers that are implementable in a sample-and-hold technique [31, Sec. 1.3]. To this end, we represent the sample behavior of (12) as system. Let $\tau > 0$, then the *sampled system* associated with (12) (and the *sampling time* τ) is given by the simple system $S_1 = (X_1, A_1, F_1)$ with $X_1 = \mathbb{R}^n$, $A_1 = U$ and for all $x \in X_1$, $a \in A_1$ we have $F_1(x, a) := \{\varphi(\tau, x, a)\}$.

A *reach and stay while avoid* specification for a sampled system (X_1, A_1, F_1) associated with (12) is parametrized by the *initial state set* $I_1 \subseteq X_1$, the *obstacles* $O_1 \subseteq X_1$ and the *target* set $Z_1 \subseteq X_1$. In particular, we would like that every element (α, ξ) of the closed behavior with initial state $\xi(0) \in I_1$ should always avoid the obstacles O_1 and eventually reach the target Z_1 and thereafter stay in Z_1 forever onwards. We express this by the specification

$$\Sigma_1 := \{(\alpha, \xi) \in (A_1 \times X_1)^{[0;T[} \mid \xi(0) \in I_1 \implies T = \infty \wedge \forall_{t \in \mathbb{Z}_+} \xi(t) \notin O_1 \wedge \exists_{t \in \mathbb{Z}_+} \forall_{t' \in [t;\infty[} \xi(t') \in Z_1\} \tag{13}$$

which we term Σ_1 *reach and stay while avoid specification* associated with (I_1, O_1, Z_1).

Given a sampled system (X_1, A_1, F_1) associated with (12) and sampling time τ, we consider a running cost function given by a combination of a function

$$g : \mathbb{R}^n \times U \to \mathbb{R} \tag{14}$$

with $g(\cdot, u)$ being continuously differentiable for all $u \in U$ and costs induced by updating the controller

$$\delta(a_1, a_1') := \begin{cases} 1 & \text{if } a_1 \neq a_1' \\ 0 & \text{if } a_1 = a_1'. \end{cases}$$

The running cost function for $S_1 = (X_1, A_1, F_1)$, for some $w \in \mathbb{R}_+$ results in

$$G_1(a_1, x_1, a_1', x_1') := \frac{1}{\tau} \int_0^\tau g(\varphi(s, x_1, a_1), a_1)\mathrm{d}s + w\delta(a_1, a_1'). \tag{15}$$

For technical reasons we introduce the modified transition function, which does not alter the control problem, given by

$$F_1(x_1, a_1) := \begin{cases} \{\varphi(\tau, x_1, a_1)\} & \text{if } x_1 \notin O_1 \\ \varnothing & \text{otherwise.} \end{cases} \tag{16}$$

We summarize the control problem as follows.

Definition 7. *A* valuated reach and stay (while avoid) *control problem associated with* (12), (14), *$\tau > 0$ and I_1, O_1, $Z_1 \subseteq \mathbb{R}^n$ is a valuated control problem (S_1, G_1, Σ_1) with $S_1 = (X_1, A_1, F_1)$, where $X_1 := \mathbb{R}^n$, $A_1 := U$ and F_1 is given by* (16). *G_1 is given by* (15) *and Σ_1 is defined in* (13).

To construct auxiliary valuated control problems for (S_1, G_1, Σ_1), we employ a notion of growth bound, which we introduced in [25], and we adapt the definition [25, Def. VIII.2] to account for the cost function g.

Definition 8. *Consider* (12), (14), *$K \subseteq \mathbb{R}^n$ and $\tau > 0$. A pair of maps $\rho\colon \mathbb{R}_+^n \times U \to \mathbb{R}_+^n$, $\gamma\colon \mathbb{R}_+^n \times U \to \mathbb{R}_+$ is a* growth bound *on $[0, \tau]$, K for* (12) *and* (14) *if $\rho(r, u) \geq \rho(r', u)$, $\gamma(r, u) \geq \gamma(r', u)$ whenever $r \geq r'$ and $u \in U$, and for every $x, x' \in K$ and $u \in U$ we have*

$$|\varphi(\tau, x', u) - \varphi(\tau, x, u)| \leq \rho(|x' - x|, u)$$

$$|\int_0^\tau g(\varphi(s, x', u), u) - g(\varphi(s, x, u), u)\mathrm{d}s| \leq \gamma(|x' - x|, u).$$

A method to compute growth bounds for (12) and (14) is given in [25] by applying [25, Thm. VIII.5] to the control system $(\dot{x}, \dot{y}) = (f(x, u), g(y, u))$.

B. Auxiliary Valuated Control Problems

The state alphabet X_2 of the auxiliary valuated control problems is given by a cover[2] of the state alphabet of the sampled system associated with (12), where the elements of the cover are non-empty, closed hyper-intervals, subsequently referred to as *cells*. We work with a subset $\bar{X}_2$ of elements of X_2. We interpret those elements as the "real" quantizer symbols and the remaining elements as overflow symbols, see [32, Sect III.A]. We assume that $\bar{X}_2$ consists of congruent cells that are uniformly aligned on a grid

$$\eta\mathbb{Z}^n = \{c \in \mathbb{R}^n \mid \exists_{k \in \mathbb{Z}^n} \forall_{i \in [1;n]}\ c_i = k_i \eta_i\} \tag{17}$$

with *grid parameter* $\eta \in (\mathbb{R}_+ \setminus \{0\})^n$, i.e.,

$$x_2 \in \bar{X}_2 \implies \exists_{c \in \eta\mathbb{Z}^n}\ x_2 = c + [\![-\eta/2, \eta/2]\!]. \tag{18}$$

[2]A cover of a set X is a set of subsets of X whose union equals X.

1) Upper Bounding Control Problem: In the construction of the auxiliary control problem $(\hat{S}_2, \hat{G}_2, \hat{\Sigma}_2)$ we follow closely the approach in [25], which we extend in this paper to account for the cost function G_1 and the specification Σ_1.

The algorithm to compute $\hat{S}_2 = (X_2, A_1, \hat{F}_2)$ is given in Alg. 1. The main loop iterates over every element in $x_2 \in X_2$ and $a \in A_1$. If x_2 is not a real quantizer symbol, the transition function is set to the empty set in line 3. Otherwise, by using the growth-bound ρ, an over-approximation D of the attainable set of (12) with respect to the cell $x_2 = c + [\![-r, r]\!] \subseteq \mathbb{R}^n$ is computed in line 7. Depending whether D is a subset of the real quantizer symbols, $\hat{F}_2$ equals D or is defined to be the empty set, see lines 8-11. The function $\hat{g}_2$ is used to define the running cost function, which results in

$$\hat{G}_2(x_2, a_2, x_2', a_2') := \tfrac{1}{\tau}\hat{g}_2(x_2, a_2) + w\delta(a_2, a_2'). \tag{19}$$

Algorithm 1 Computation of $\hat{F}_2$ and $\hat{g}_2$

Require: X_2, A_1, ρ, φ, g, $r = \eta/2$, τ

1: **for all** $x_2 \in X_2$ and $a \in A_1$ **do**
2:   **if** $x_2 \notin \bar{X}_2$ **then**
3:     $\hat{F}_2(x_2, a) := \varnothing$, $\hat{g}_2(x_2, a) := \infty$
4:   **else** let $c + [\![-r, r]\!] = x_2$
5:     $r' := \rho(r, a)$
6:     $c' := \varphi(\tau, c, a)$
7:     $D := \{x_2' \in X_2 \mid (c' + [\![-r', r']\!]) \cap x_2' \neq \varnothing\}$
8:     **if** $D \subseteq \bar{X}_2$ **then**
9:       $\hat{F}_2(x_2, a) := D$
10:     **else**
11:       $\hat{F}_2(x_2, a) := \varnothing$
12:     $\hat{g}_2(x_2, a) := \int_0^\tau g(\varphi(s, c, a), a)\mathrm{d}s + \gamma(r, a)$

The specification $\hat{\Sigma}_2$ for $\hat{S}_2$ follows as reach avoid while stay specification associated with the sets $(\hat{I}_2, \hat{O}_2, \hat{Z}_2)$ given by

$$\hat{Z}_2 := \{x_2 \in X_2 \mid x_2 \subseteq Z_1\},\ \hat{I}_2 := \{x_2 \in X_2 \mid x_2 \cap I_1 \neq \varnothing\}$$
$$\hat{O}_2 := \{x_2 \in X_2 \mid x_2 \cap O_1 \neq \varnothing\}. \tag{20}$$

Theorem 3. *Let (S_1, G_1, Σ_1) with $S_1 = (X_1, A_1, F_1)$ be a valuated reach and stay control problem associated with* (12), (14), *$\tau > 0$ and I_1, O_1, $Z_1 \subseteq \mathbb{R}^n$. Let X_2 be a cover of X_1 by non-empty, closed hyper-intervals. Consider a subset $\bar{X}_2 \subseteq X_2$ that satisfies* (18) *and let ρ,γ be a growth bound on $[0, \tau]$ and $\cup_{x_2 \in \bar{X}_2} x_2$ associated with* (12) *and* (14) *(cf. Definition 8). Consider $\hat{S}_2 = (X_2, A_1, \hat{F}_2)$ with $\hat{F}_2$ given according to Alg. 1 and $\hat{G}_2$ according to* (19). *Let $\hat{\Sigma}_2$ be the reach avoid while stay specification associated with the sets $(\hat{I}_2, \hat{O}_2, \hat{Z}_2)$ that are defined in* (20). *Then we have*

$$(S_1, G_1, \Sigma_1) \preccurlyeq_{Q_e} (\hat{S}_2, \hat{G}_2, \hat{\Sigma}_2)$$

where $Q_e := \{(x_1, x_2, a_1, a_2) \mid x_1 \in x_2 \wedge a_1 = a_2\}$.

2) Lower Bounding Control Problem: The construction of the auxiliary problem $(\check{S}_2, \check{G}_2, \check{\Sigma}_2)$ to obtain a lower bound on the value function of (S_1, G_1, Σ_1) follows along the lines of the previous section. The state alphabet of the system $\check{S}_2 = (X_2, A_1 \times X_2, \check{F}_2)$ is again given by X_2. However, compared to the construction of $\hat{F}_2$, in which we treated the non-determinism as adversarial, we treat the non-determinism as controllable, i.e., the input alphabet is given by $A_1 \times X_2$ and the controller can pick the successor state in the over-approximation of the attainable set, see Alg. 2, lines 8-9. The definition of $\check{G}_2$ follows from the function $\check{g}_2$ which is computed in line 3 and 10. The running cost function follows

$$\check{G}_2(x_2, (a_2, \bar{x}_2), x_2', (a_2', \bar{x}_2')) := \tfrac{1}{\tau}\check{g}_2(x_2, a_2) + w\delta(a_2, a_2'). \tag{21}$$

Algorithm 2 Computation of $\check{F}_2$ and $\check{g}_2$

Require: X_2, A_1, ρ, φ, g, $r = \eta/2$, τ

1: **for all** $x_2 \in X_2$ and $a \in A_1$ **do**
2:   **if** $x_2 \notin \bar{X}_2$ **then**
3:     $\check{F}_2(x_2, a) := \varnothing$, $\check{g}_2(x_2, a) := -\infty$
4:   **else** let $c + [\![-r, r]\!] = x_2$
5:     $r' := \rho(r, a)$
6:     $c' := \varphi(\tau, c, a)$
7:     $D := \{x_2' \in X_2 \mid (c' + [\![-r', r']\!]) \cap x_2' \neq \varnothing\}$
8:     **for all** $x_2' \in D$ **do**
9:       $\check{F}_2(x_2, (a, x_2')) := \{x_2'\}$
10:     $\check{g}_2(x_2, a) := \int_0^\tau g(\varphi(s, c, a), a)\mathrm{d}s - \gamma(r, a)$

The specification $\check{\Sigma}_2$ for $\check{S}_2$ is a reach avoid while stay specification associated with the sets $(\check{I}_2, \check{O}_2, \check{Z}_2)$ given by

$$\begin{aligned}&\check{I}_2 := \{x_2 \in X_2 \mid x_2 \subseteq I_1\},\ \check{O}_2 := \{x_2 \in X_2 \mid x_2 \subseteq O_1\},\\ &\check{Z}_2 := \{x_2 \in X_2 \mid x_2 \cap Z_1 \neq \varnothing\}.\end{aligned} \tag{22}$$

The following theorem parallels Theorem 3, where we additionally have to assume that the real quantizer symbols $\bar{X}_2$ (exclusively) cover the domain of the control problem $O_1^c := \mathbb{R}^n \smallsetminus O_1$. We express this by

$$x_1 \in O_1^c \wedge x_1 \in x_2 \in X_2 \implies x_2 \in \bar{X}_2. \tag{23}$$

Theorem 4. *Let* (S_1, G_1, Σ_1) *with* $S_1 = (X_1, A_1, F_1)$ *be a valuated reach and stay control problem associated with* (12), (14), $\tau > 0$ *and* $I_1, O_1, Z_1 \subseteq \mathbb{R}^n$. *Let* X_2 *be a cover of* X_1 *by non-empty, closed hyper-intervals. Consider a subset* $\bar{X}_2 \subseteq X_2$ *that satisfies* (18) *and* (23). *Let* ρ,γ *be a growth bound on* $[0, \tau]$ *and* $\cup_{x_2 \in \bar{X}_2} x_2$ *associated with* (12) *and* (14). *Consider* $\check{S}_2 = (X_2, (A_1, X_2), \check{F}_2)$ *with* $\check{F}_2$ *given according to Alg. 2 and* $\check{G}_2$ *according to* (21). *Let* $\check{\Sigma}_2$ *be the reach avoid while stay specification associated with the sets* $(\check{I}_2, \check{O}_2, \check{Z}_2)$ *that are defined in* (22). *Then we have*

$$(\check{S}_2, \check{G}_2, \check{\Sigma}_2) \preceq_{R_e} (S_1, G_1, \Sigma_1)$$

where $R_e := \{(x_2, x_1, (a_2, x_2'), a_1) \mid x_1 \in x_2 \wedge a_1 = a_2\}$.

VI. A Numerical Example

We provide a small numerical example. We synthesize a controller to regulate the temperature in a room. The control system is given by the scalar differential equation

$$\dot{\xi}(t) = \tfrac{1}{200}(t_e - \xi(t)) + \tfrac{1}{100}(t_h - \xi(t))a, \quad a \in \{0, 1\} \tag{24}$$

where $t_e = 10^\circ$ and $t_h = 50^\circ$ is the outside temperature, respectively, the heater temperature in Celsius. The control input equals $a = 1$ if the heater is on and $a = 0$ if the heater is off. The sampling time is fixed to $\tau = 5\,\mathrm{sec}$. The parameters are taken from [33]. The aim is to design a controller such that the temperature evolves in the range of $Z_1 := [18, 22]^\circ$ Celsius. We fix the domain of the problem to $O_1^c := [15, 25]^\circ$ so that the obstacles result in $O_1 := \mathbb{R} \smallsetminus O_1^c$ and the set of the initial states is defined by $I_1 := [15.5, 24.5]$. We use $h(x) := \frac{2}{100}\big(\log(1+\mathrm{e}^{100x}) - \log(2)\big) - x$ as a smooth approximation of the absolute value. Then we consider the running costs given by (15) with

$$g(x, u) := \tfrac{(1-w)}{20} h(21 - \varphi(t, x, u))$$

with which we penalize the deviation of the temperature from the desired set point of 21°. We apply [25, Thm. VIII.5] and obtain a growth bound (valid on any $[0, \tau]$ and $K \subseteq \mathbb{R}$) by $\rho(r, u) := \mathrm{e}^{-\frac{3}{200}\tau} r$ and $\gamma(r, u) := (1 - w)10/3r$. Here we used the fact that the absolute value of the derivative of h is bounded, i.e., $|h'(x)| \leq 1$ for all $x \in \mathbb{R}$.

We construct a valuated control problem $(\hat{S}_2, \hat{G}_2, \hat{\Sigma}_2)$ according to Theorem 3. We fix the grid parameter to $\eta = 0.01$ and define the real quantizer symbols by $\bar{X}_2 := \{c + [-\eta/2, \eta/2] \mid c \in \eta\mathbb{Z}, c + [\eta/2, \eta/2] \cap O_1^c \neq \varnothing\}$. A cover of $\mathbb{R}$ results by $X_2 := \bar{X}_2 \cup O_1$. We approach the solution of the control problem $(\hat{S}_2, \hat{\Sigma}_2)$ in two steps. First, we focus on the target region $\hat{Z}_2$ and synthesize a controller to enforce the safety specification

$$\hat{\Sigma}_s := \big\{(\hat{\alpha}, \hat{\xi}) \in (A_1 \times \hat{X}_2)^{[0;T[} \mid \hat{\xi}(0) \in \nu\hat{Z}_2 \implies T = \infty \wedge \forall_{t \in \mathbb{Z}_+} \hat{\xi}(t) \in \hat{Z}_2\big\}.$$

Here $\nu\hat{Z}_2$ is the maximal controller invariant set contained in $\hat{Z}_2$, which we obtain in the synthesis process. We fix a value $\hat{K}_2 \in \mathbb{R}$ and follow the approach in [20] to synthesize a controller $\hat{C}_s$ that solves $(\hat{S}_2, \hat{\Sigma}_s)$ and whose associate cost function $\hat{J}_2$ is bounded by $\hat{K}_2$ for all $\hat{x}_2 \in \nu\hat{Z}_2$. In the second step, we follow the approach in [25, Sec. IX] and synthesize a controller $\hat{C}_r$ to enforce the reach avoid specification

$$\big\{(\hat{\alpha}, \hat{\xi}) \in (A_1 \times \hat{X}_2)^\infty \mid \hat{\xi}(0) \in \hat{I}_2 \implies \forall_{t \in \mathrm{dom}\,\hat{\xi}} \hat{\xi}(t) \in \hat{O}_2 \wedge \exists_{t \in \mathrm{dom}\,\hat{\xi}} \hat{\xi}(t) \in \nu\hat{Z}_2\big\}.$$

Given $\hat{C}_s$, $\nu\hat{Z}_2$ and $\hat{C}_r$ it is straightforward to construct a controller $\hat{C}_2$ which solves $(\hat{S}_2, \hat{\Sigma}_2)$. Moreover, the associated cost function is bounded by $\hat{K}_2$. We apply Theorem 1 and see that $\hat{C}_2 \circ Q$ solves (S_1, Σ_1) and $\hat{K}_2$ provides an upper bound on the associated cost function J_1. We synthesize two controllers, one for running costs with weight $w = 0$ and one for $w = 1$. For $w = 0$ and $w = 1$ we were able to obtain a bound on the cost function by $\hat{K} = 0.04$, respectively,

$\hat{K} = 0.2$. Two closed loop signals, each from a different controller, together with the cumulative costs $L_1(t, \alpha, \xi)$, are illustrated in Fig. 2.

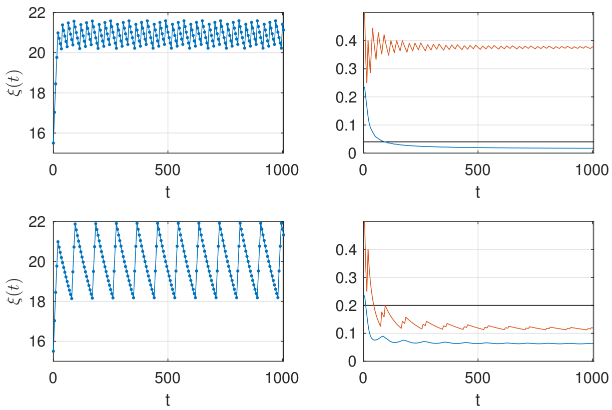

Fig. 2. Left: Two closed loop signals with initial state $x_1 = 15.5°$ resulting from two controllers synthesized with running cost weight $w = 0$ (upper subplot) and $w = 1$ (lower subplot). Right: Cumulative costs $L_1(t, \alpha, \xi)$ for $w = 1$ (*red*) and $w = 0$ (*blue*). The dark black lines depict the theoretical bound $\hat{K}_2$.

We conducted the experiments on a Intel 1.3GHz CPU with 8GB memory. We used SCOTS [34] to compute the symbolic models and algorithms in [20] to solve the synthesis problem with average cost objectives. None of the computations took more than two seconds.

References

[1] R. Bellman. "Dynamic programming and Lagrange multipliers". In: *PNAS* 42.10 (1956), pp. 767–769.

[2] R. E. Kalman. "Contributions to the theory of optimal control". In: *Bol. Soc. Mat. Mexicana* 5.2 (1960), pp. 102–119.

[3] R. A. Freeman and P. V. Kokotović. *Robust nonlinear control design: state-space and Lyapunov techniques*. Birkäuser, 1996.

[4] A. Church. "Logic, arithmetic and automata". In: *Proc. of the Int. Congress of Mathematicians*. 1962, pp. 23–35.

[5] M. O. Rabin. "Automata on infinite objects and Church's problem". In: Conf. Board of the Math. Sci. 1972.

[6] A. E. Emerson and E. M. Clarke. "Using branching time temporal logic to synthesize synchronization skeletons". In: *Science of Computer Programming* 2.3 (1982), pp. 241–266.

[7] A. Pnueli and R. Rosner. "On the Synthesis of a Reactive Module". In: *ACM POPL*. 1989, pp. 179–190.

[8] E. M. Wolff, U. Topcu, and R. M. Murray. "Optimal Control with Weighted Average Costs and Temporal Logic Specifications". In: *Robotics: Science and Systems*. 2012.

[9] M. Mazo and P. Tabuada. "Symbolic approximate time-optimal control". In: *Systems & Control Letters* (2011), pp. 256–263.

[10] A. Girard. "Controller synthesis for safety and reachability via approximate bisimulation". In: *Automatica* 48.5 (2012), pp. 947–953.

[11] G. Reissig and M. Rungger. "Abstraction-based solution of optimal stopping problems under uncertainty". In: *IEEE CDC*. 2013, pp. 3190–3196.

[12] F. de Roo and M. Mazo. "On symbolic optimal control via approximate simulation relations". In: *IEEE CDC*. 2013, pp. 3205–3210.

[13] X. Ding, S. L. Smith, C. Belta, and D. Rus. "Optimal control of Markov decision processes with linear temporal logic constraints". In: *IEEE TAC* 59.5 (2014), pp. 1244–1257.

[14] E. A. Gol, M. Lazar, and C. Belta. "Temporal logic model predictive control". In: *Automatica* 56 (2015), pp. 78–85.

[15] K. Chatterjee, T. A. Henzinger, and M. Jurdziński. "Mean-payoff parity games". In: *IEEE LICS*. 2005, pp. 178–187.

[16] R. Bloem, K. Chatterjee, T. A. Henzinger, and B. Jobstmann. "Better quality in synthesis through quantitative objectives". In: *CAV*. Springer. 2009, pp. 140–156.

[17] K. Chatterjee and L. Doyen. "Energy parity games". In: *Automata, Languages and Programming*. Springer, 2010, pp. 599–610.

[18] K. Chatterjee, L. Doyen, and T. A. Henzinger. "Quantitative languages". In: *ACM TOCL* 11.4 (2010), 23:1–23:38.

[19] P. Černỳ, K. Chatterjee, T. A. Henzinger, A. Radhakrishna, and R. Singh. "Quantitative synthesis for concurrent programs". In: *CAV*. Springer. 2011, pp. 243–259.

[20] A. Bohy, V. Bruyere, E. Filiot, and J.-F. Raskin. "Synthesis from LTL specifications with mean-payoff objectives". In: *Tools and Algorithms for the Construction and Analysis of Systems*. Springer, 2013, pp. 169–184.

[21] D. P. Bertsekas. *Dynamic programming and optimal control*. Vol. 1 & 2. Athena Scientific, 1995.

[22] A. Ehrenfeucht and J. Mycielski. "Positional strategies for mean payoff games". In: *International Journal of Game Theory* 8.2 (1979), pp. 109–113.

[23] U. Zwick and M. Paterson. "The complexity of mean payoff games on graphs". In: *Theoretical Computer Science* 158.1 (1996), pp. 343–359.

[24] P. Tabuada. *Verification and control of hybrid systems*. New York: Springer, 2009.

[25] G. Reißig, A. Weber, and M. Rungger. "Feedback Refinement Relations for the Synthesis of Symbolic Controllers". In: *IEEE TAC* 62 (2017). DOI: 10.1109/TAC.2016.2593947.

[26] G. Reißig and M. Rungger. *Symbolic Optimal Control*. 2016. URL: http://arxiv.org/.

[27] P.-J. Meyer, A. Girard, and E. Witrant. "Safety control with performance guarantees of cooperative systems using compositional abstractions". In: *IFAC-PapersOnLine* 48.27 (2015), pp. 317–322.

[28] R. T. Rockafellar and R. J.-B. Wets. *Variational analysis*. Vol. 317. 3rd corr printing 2009. Springer, 1998.

[29] M. Mazo, A. Davitian, and P. Tabuada. "Pessoa: A tool for embedded controller synthesis". In: *Computer Aided Verification*. Springer. 2010, pp. 566–569.

[30] S. Tripakis, B. Lickly, T. A. Henzinger, and E. A. Lee. "A theory of synchronous relational interfaces". In: *ACM Transactions on Programming Languages and Systems* 33.4 (2011), p. 14.

[31] E. D. Sontag. *Mathematical control theory: deterministic finite dimensional systems*. 2nd Edition. Springer, 1998.

[32] G. Reissig. "Computing abstractions of nonlinear systems". In: *IEEE TAC* 56.11 (2011), pp. 2583–2598.

[33] S. Mouelhi, A. Girard, and G. Gössler. "CoSyMA: a tool for controller synthesis using multi-scale abstractions". In: *HSCC*. ACM. 2013, pp. 83–88.

[34] M. Rungger and M. Zamani. "SCOTS: A Tool for the Synthesis of Symbolic Controllers". In: *HSCC*. ACM, 2016.