This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2018.2863178, IEEE Transactions on Automatic Control

Symbolic Optimal Control

Gunther Reissig and Matthias Rungger

***Abstract*—We present novel results on the solution of a class of leavable, undiscounted optimal control problems in the minimax sense for nonlinear, continuous-state, discrete-time plants. The problem class includes entry-(exit-)time problems as well as minimum time, pursuit-evasion and reach-avoid games as special cases. We utilize auxiliary optimal control problems ("abstractions") to compute both upper bounds of the value function, i.e., of the achievable closed-loop performance, and symbolic feedback controllers realizing those bounds. The abstractions are obtained from discretizing the problem data, and we prove that the computed bounds and the performance of the symbolic controllers converge to the value function as the discretization parameters approach zero. In particular, if the optimal control problem is solvable on some compact subset of the state space, and if the discretization parameters are sufficiently small, then we obtain a symbolic feedback controller solving the problem on that subset. These results do not assume the continuity of the value function or any problem data, and they fully apply in the presence of hard state and control constraints.**

I. Introduction

In this paper we present novel results on the solution of optimal control problems, in which we follow a symbolic synthesis approach [1]–[3] and utilize finite, auxiliary problems ("abstractions") obtained from discretizing the original problem data. Our theory provides symbolic feedback controllers, and it culminates in novel convergence and completeness results including the following: If the optimal control problem is solvable on some compact subset of the state space, and if the discretization parameters are sufficiently small, then the obtained controller solves the problem on that subset.

More specifically, we consider discrete-time control systems that are defined by difference inclusions of the form

$$x(t+1) \in F(x(t), u(t)), \tag{1}$$

where $x(t) \in X$ and $u(t) \in U$ represents the *state* and the *input signal*, respectively. Typically, the sets X and U are uncountably infinite. We use set-valued *transition functions* $F\colon X \times U \rightrightarrows X$ to account for possible perturbations such as actuator inaccuracies and modeling uncertainties; see e.g. [2]. The problem data also includes non-negative, extended real-valued *running* and *terminal cost functions*, g and G,

$$g\colon X \times X \times U \to \mathbb{R}_+ \cup \{\infty\}, \tag{2a}$$

$$G\colon X \to \mathbb{R}_+ \cup \{\infty\}, \tag{2b}$$

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

M. Rungger is with the Hybrid Control Systems Group at the Department of Electrical and Computer Engineering at the Technical University of Munich, Germany.

This work has been supported by the German Research Foundation (DFG) under grant no. RE 1249/4-1.

where $\mathbb{R}_+$ denotes the set of non-negative reals. As we demonstrate in Section VIII, infinite costs are useful to represent hard actuation and state constraints.

Given the aforementioned problem data, we investigate optimal control problems where the evolution of the closed-loop must be stopped at some finite, but not predetermined, time. At that point, the *total cost* is determined as the sum of the terminal cost and the previously accumulated running costs. We seek to synthesize a feedback controller that minimizes, or approximately minimizes, the total cost in the minimax (worst-case) sense, in which the controller generates both an input signal for the plant (1) and additionally a signal that determines the stopping time. In particular, the considered optimal control problem is *leavable* as the controller is allowed to stop the evolution of the closed-loop at any time [4]. In contrast to similar settings, in our problem stopping is mandatory and not discretionary, and we penalize non-stopping evolutions with infinite costs. The problem class is formally defined in Section III-A and includes entry-(or exit-)time problems as well as minimum time, pursuit-evasion and reach-avoid games as special cases. Examples are given in Sections III-B and VIII.

Outline of the Proposed Approach. We follow a symbolic synthesis approach [1]–[3]: First, an *abstraction*, i.e., a finite, auxiliary optimal control problem, is constructed by discretizing the problem data. Second, a controller solving the auxiliary problem is synthesized, and third, the latter controller is refined to obtain a controller for the original problem. In this context, we label quantities and objects that are defined with respect to the original and to the auxiliary optimal control problem as *concrete* and *abstract*, respectively.

In our theory, abstractions shall be constructed so that the abstract *value function*, i.e., the best achievable performance of the abstract closed-loop, provides an upper bound of the concrete value function. Conforming to the correct-by-construction paradigm of the symbolic approach, the theory also guarantees that the *closed-loop value function* associated with the abstract controller, i.e., the worst-case performance of that controller used in the abstract closed loop, provides an upper bound of the closed-loop value function associated with the concrete controller.

Since even rather coarse discretizations of the problem data may very well qualify as abstractions, the abstract value function will provide a rather conservative bound on the concrete value function, in general. To resolve that issue, we shall introduce a suitable notion of *conservatism* for abstractions, which is closely related to the accuracy by which the problem data is discretized. As our main results, we shall establish the convergence of both of the aforementioned upper bounds to the concrete value function as the conservatism of the abstraction approaches zero. In turn, as we shall also show, our synthesis approach is complete in the following sense: If the original optimal control problem is solvable on a compact subset of the state space, then the obtained controller solves the original problem on that subset whenever a sufficiently precise abstraction is employed.

Our results do not assume the continuity of the value function or any problem data, and they fully apply in the presence of hard state and control constraints. The resulting feedback controllers are memoryless, finitely representable and symbolic, i.e., they require only quantized as opposed to full state information.

Related Work. The symbolic synthesis scheme has been applied to a variety of optimal control problems including minimum time problems [5], [6], entry-time problems [7], [8] and finite horizon problems [9]. Optimality properties in combination with regular language specifications are analyzed in [10]. The results in [5], [7] are based on approximate alternating simulation relations. As discussed in detail in [2, Sec. IV], this leads to overly complex, dynamic controllers which additionally require full state information. The controllers synthesized in [6] also require full state information. Moreover, while the works [8]–[10] lead to arbitrarily close approximations of value functions, the respective convergence results do not account for perturbations [8]–[10], do not apply in the presence of hard constraints and discontinuous value functions [8], [9], or require piecewise linear plant dynamics [10]. Additionally, the approach in [8] relies on the ability to exactly determine first integrals of the plant dynamics, and the one in [10], on the ability to verify a non-trivial property for an exact optimal solution (which is assumed to exist).

Closely related to our approach is the numerical approximation of the value function, which has a rich history and has been a major research focus since the early days of Dynamic Programming [11]. Related convergence results for deterministic finite and infinite horizon optimal control problems can be found in [12]–[18], and for several classes of stochastic optimal control problems, in [19]–[22]. Convergence results for leavable deterministic optimal control problems (or deterministic optimal stopping problems), as considered in this paper, are presented in [23]–[28]. The vast majority of works focus on the special cases of minimum time [25], [26] and entry-(or exit-)time problems [27], [28] or on discounted running costs [24], or apply only to continuous-time problems [24]–[26]. Additionally, these works do not account for perturbations [23], [24], or do not apply in the presence of hard constraints [23], [25] and discontinuous value functions [23], [27]. While the works [25], [26], [28] do account for discontinuous value functions, the respective results do not lead to controllers whose closed-loop performances arbitrarily closely approximate the value function.

Another line of related research originates from the extension of asymptotically optimal sampling-based motion planing [29] to kinodynamic planning that takes nonlinear dynamics into account [30]. In contrast to our approach, the goal is not to synthesize optimal feedback controllers, but to find an open-loop input signal that optimally steers the system from a fixed initial state to fixed final state or final region. Consequently, perturbations cannot be considered. In addition, the convergence results in [30] are probabilistic and do not provide worst-case guarantees.

Summary of Contributions. In view of the preceding discussion, we summarize our contributions as follows. Firstly, we characterize the value function as the maximal fixed point of an appropriately defined Dynamic Programming operator. A detailed comparison with related results is provided in Section IV. Secondly, we propose a correct-by-construction approach to synthesize memoryless symbolic controllers requiring only quantized state information, as well as guarantees in the form of upper bounds on the controllers' worst-case performances, for general classes of plant dynamics and cost functions (Section V). Thirdly, and most importantly, we establish powerful convergence and completeness results (Section VI), which imply that even in the presence of hard constraints and discontinuous value functions, our method is capable of synthesizing controllers whose performance guarantees arbitrarily closely approximate the best achievable performance. In Section VIII, we demonstrate our approach on three examples.

For the sake of self-consistency of the paper, we present in Section VII our method from [31] to compute abstractions for a class of sampled control systems, and we also present an algorithm to efficiently solve auxiliary, abstract optimal control problems. In the Appendix we collect some auxiliary results numbered A.1 through A.5. Preliminary versions of some of the results in this paper have been announced in [32].

II. Preliminaries

The relative complement of the set A in the set B is denoted by $B \setminus A$. $\mathbb{R}$, $\mathbb{R}_+$, $\mathbb{Z}$ 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 $x \in \mathbb{R}$. $[a,b]$, $]a,b[$, $[a,b[$, and $]a,b]$ denote closed, open and half-open, respectively, intervals with end points a and b, e.g. $[0,\infty[= \mathbb{R}_+$. $[a;b]$, $]a;b[$, $[a;b[$, and $]a;b]$ stand for discrete intervals, e.g. $[a;b] = [a,b] \cap \mathbb{Z}$, $[1;4[= \{1,2,3\}$, and $[0;0[= \varnothing$. $\max M$, $\min M$, $\sup M$ and $\inf M$ denote the maximum, the minimum, the supremum and the infimum, respectively, of the nonempty subset $M \subseteq [-\infty,\infty]$, and we adopt the convention that $\sup \varnothing = 0$.

$f \colon A \rightrightarrows B$ denotes a *set-valued map* from the set A into the set B, whereas $f \colon A \to B$ denotes an ordinary map; see [33]. The set of maps $A \to B$ is denoted B^A. 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.

We identify set-valued maps $f \colon A \rightrightarrows B$ with binary relations on $A \times B$, i.e., $(a,b) \in f$ iff $b \in f(a)$. Moreover, if f is single-valued, it is identified with an ordinary map $f \colon A \to B$. The restriction of f to a subset $M \subseteq A$ is denoted $f|_M$. The inverse mapping $f^{-1} \colon B \rightrightarrows A$ is defined by $f^{-1}(b) = \{a \in A \,|\, b \in f(a)\}$, $f \circ g$ denotes the composition of f and g, $(f \circ g)(x) = f(g(x))$, and the image of a subset $C \subseteq A$ under f is denoted $f(C)$, $f(C) = \bigcup_{a \in C} f(a)$.

If A and B are metric spaces, then f is *upper semi-continuous* (u.s.c.) if $f^{-1}(\Omega)$ is closed for every closed subset $\Omega \subseteq B$. Alternatively, if $B = [-\infty,\infty]$, then f is *bounded* on the subset $C \subseteq A$ if $f(C)$ is a bounded subset of $\mathbb{R}$.

For maps $f, g \colon X \to [-\infty,\infty]$, the relations $<$, $\leq$, $\geq$, $>$ are defined point-wise, e.g. $f < g$ if $f(x) < g(x)$ for all

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2018.2863178, IEEE Transactions on Automatic Control

$x \in X$. Analogously, the relations are interpreted component-wise for elements of $[-\infty, \infty]^n$. The set of minimum points of f in some subset $Q \subseteq X$ is denoted $\operatorname{argmin}\{f(x) \mid x \in Q\}$. $\operatorname{hypo} f = \{(x, \gamma) \in X \times \mathbb{R} \mid \gamma \leq f(x)\}$ is the *hypograph* of f, and f is u.s.c. if X is a metric space and $\operatorname{hypo} f \subseteq X \times \mathbb{R}$ is closed [33], [34].

The *backward shift operator* σ is defined as follows. If the map f is defined on $[0; T[$ for some $T \in \mathbb{N} \cup \{\infty\}$, then σf is the map defined on $[0; T-1[$ and given by $(\sigma f)(t) = f(t+1)$.

III. A Leavable Optimal Control Problem

We develop our theory in a rather general setting, and for now we simply assume that X and U are nonempty sets. These assumptions already allow for a fixed-point characterization of the value function. As we progress with our analysis we gradually impose stricter assumptions. In particular, we demonstrate the upper semi-continuity of the value function under assumptions including that X and U are metric spaces. Here the abstract treatment of X and U is crucial. Even if the original system evolves in $\mathbb{R}^n$, the abstractions we shall construct do not. Similarly, to prove our main results in Section VI, we will need to construct yet another auxiliary problem with a non-euclidean state alphabet. Moreover, our setting covers plants whose states naturally form finite-dimensional manifolds, which is common in e.g. robot dynamics [35].

A. Problem definition

We seek to control *systems* whose dynamics is defined by difference inclusions of the form (1). Subsequently, we often refer to these systems as *plants*. Controllers, on the other hand, are defined by more general inclusions of the form

$$(z(t+1), u(t), v(t)) \in H(z(t), x(t)), \tag{3}$$

where z represents the state of the controller. The controller accepts a state signal x of the plant as its input and generates a signal u that serves as input for the plant. See Fig. 1. The controller additionally generates a stopping signal v which is used to terminate the evolution of the closed loop and will be discussed in conjunction with our definition of cost functionals. We formalize the aforementioned concepts below.

III.1 Definition. A *system* is a triple

$$(X, U, F), \tag{4}$$

where X and U are nonempty sets and $F\colon X \times U \rightrightarrows X$ is strict. A pair $(u, x) \in U^{\mathbb{Z}_+} \times X^{\mathbb{Z}_+}$ is a *solution* of the system (4) if (1) holds for all $t \in \mathbb{Z}_+$.

A *controller* for the system (4) is a quintuple

$$(Z, Z_0, \widetilde{X}, \widetilde{U}, H), \tag{5}$$

where Z, Z_0, $\widetilde{X}$, $\widetilde{U}$ are non-empty sets, $Z_0 \subseteq Z$, $X \subseteq \widetilde{X}$, $\widetilde{U} \subseteq U$, and $H\colon Z \times \widetilde{X} \rightrightarrows Z \times \widetilde{U} \times \{0,1\}$ is strict. A controller (5) is *static* if Z is a singleton. A quadruple $(u, v, z, x) \in \widetilde{U}^{\mathbb{Z}_+} \times \{0,1\}^{\mathbb{Z}_+} \times Z^{\mathbb{Z}_+} \times \widetilde{X}^{\mathbb{Z}_+}$ is a *solution* of the controller (5) if $z(0) \in Z_0$ and (3) holds for all $t \in \mathbb{Z}_+$. □

We use $C \in \mathcal{F}(X, U)$ to denote the fact that C is a controller for the system (4). The sets X and Z are the *state alphabet*, Z_0 is the *initial state alphabet*, U and $\widetilde{X}$ are the *input alphabet*, and the maps F and H are the *transition function*, of the system (4) and the controller (5), respectively.

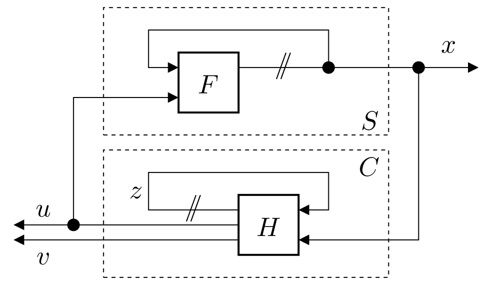

Figure 1. Closed loop $C \times S$ according to Definition III.2. The symbol $/\!/$ denotes a delay.

We emphasize that our notion of controller is equivalent to the respective notion in [2] in the non-blocking case, and it subsumes related notions from the literature, such as *causal feedback strategy* [36, Ch. VIII], *control strategy* [37], *feedback plan* [38], and *policy* [12]. Specifically, any strict policy $\mu\colon Z \times X \rightrightarrows U \times \{0,1\}$ with $Z = \bigcup_{T \in \mathbb{Z}_+} U^{[0;T[} \times X^{[0;T[}$, which generates signals u and v according to

$$(u(t), v(t)) \in \mu(u|_{[0;t[}, x|_{[0;t[}, x(t))$$

in place of (3), can be equivalently represented by a controller with state alphabet Z. On the other hand, as we shall see later, static (or *memoryless*) controllers are sufficient to approximately solve the optimal control problems investigated in the present paper, to arbitrary accuracy.

III.2 Definition. Let S denote the system (4) and suppose that $C \in \mathcal{F}(X, U)$, where C is of the form (5).

The *behavior* $\mathcal{B}(C \times S) \subseteq (U \times \{0,1\} \times X)^{\mathbb{Z}_+}$ of the closed-loop composed of C and S is defined by the requirement that $(u, v, x) \in \mathcal{B}(C \times S)$ iff there exists a signal $z\colon \mathbb{Z}_+ \to Z$ such that (u, v, z, x) is a solution of C and (u, x) is a solution of S. In addition, the *behavior initialized at* $p \in X$ is denoted by $\mathcal{B}_p(C \times S)$ and defined by $\mathcal{B}_p(C \times S) = \{(u, v, x) \in \mathcal{B}(C \times S) \mid x(0) = p\}$. □

Our problem data also includes a *running cost function* g and a *terminal cost function* G as in (2). The total cost to be minimized is then given by the *cost functional* $J\colon (U \times \{0,1\} \times X)^{\mathbb{Z}_+} \to [0, \infty]$, which is defined as the sum of the terminal cost and accumulated running costs, i.e.,

$$J(u, v, x) = G(x(T)) + \sum_{t=0}^{T-1} g(x(t), x(t+1), u(t)) \tag{6a}$$

if $v \neq 0$ and $T = \min v^{-1}(1)$, and otherwise we define J by

$$J(u, v, x) = \infty. \tag{6b}$$

Throughout the paper, we identify the optimal control problem with its problem data and use the following definition.

III.3 Definition. An *optimal control problem* is a tuple

$$(X, U, F, G, g), \tag{7}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2018.2863178, IEEE Transactions on Automatic Control

where (4) is a system and G and g are non-negative extended real-valued functions as in (2). □

The notions of state alphabet, input alphabet and transition function are carried over from the system (4) to the optimal control problem (7) in the obvious way.

As already indicated, solving the problem (7) means to find controllers $C \in \mathcal{F}(X, U)$ which, for every state $p \in X$, minimize or approximately minimize the cost (6) for $(u, v, x) \in \mathcal{B}_p(C \times S)$ in a worst-case sense, where S denotes the plant (4). Here, the stopping signal $v \colon \mathbb{Z}_+ \to \{0, 1\}$ determines, by its first 0-1 edge, the instance of time when the optimization process stops and the terminal costs are evaluated, and the worst-case cost is given by the *closed-loop value function* $L \colon X \to [0, \infty]$ of (7) associated with C,

$$L(p) = \sup_{(u,v,x)\in\mathcal{B}_p(C\times S)} J(u, v, x). \tag{8}$$

It follows that the achievable closed-loop performance is determined by the *value function* $V \colon X \to [0, \infty]$ of (7),

$$V(p) = \inf_{C\in\mathcal{F}(X,U)} \sup_{(u,v,x)\in\mathcal{B}_p(C\times S)} J(u, v, x). \tag{9}$$

As we show in Theorem IV.1, the value function satisfies

$$V(p) = \sup_{\beta\in\Delta(p)} \inf_{u\in U^{\mathbb{Z}_+}} \inf_{v\in\{0,1\}^{\mathbb{Z}_+}} J(u, v, \beta(u)) \tag{10}$$

for all $p \in X$, where $\Delta(p)$ is the set of all strictly causal maps $\beta \colon U^{\mathbb{Z}_+} \to X^{\mathbb{Z}_+}$ for which $(u, \beta(u))$ is a solution of S satisfying $\beta(u)(0) = p$, for every $u \in U^{\mathbb{Z}_+}$. Here, β is *causal* (resp., *strictly causal*) if $\beta(u)|_{[0;T]} = \beta(\tilde{u})|_{[0;T]}$ whenever $u, \tilde{u} \in U^{\mathbb{Z}_+}$, $T \in \mathbb{Z}_+$ and $u|_{[0;T]} = \tilde{u}|_{[0;T]}$ (resp., $u|_{[0;T[} = \tilde{u}|_{[0;T[}$). Thus, in terms of performance, our concept of controller is equivalent to *non-anticipating strategies* [28].

B. Important Special Cases

We briefly discuss special cases of the class of optimal control problems considered in this paper. For further examples, including an entry-(or exit-)time problem and a problem whose underlying dynamics is chaotic, see Section VIII.

III.4 Example (Shortest Path Problem). Given a directed graph, we wish to find shortest paths from a specified source vertex to all other vertices [39]. This problem and its generalizations have numerous applications [28], [39]–[41]. For a formal description, let X and $A \subseteq X \times X$ be finite sets of vertices and of arcs, respectively, of a directed graph, and let $s \in X$ be a distinguished source vertex. Let a non-negative length $w_{p,q}$ be associated with each arc (p, q), i.e., $w \colon A \to \mathbb{R}_+$, and define the length of a path as the sum of the lengths of its arcs. The distance from s to $p \in X$, denoted $d(p)$, is the minimum length of any (directed) path from s to p, and is defined to be ∞ if no such path exists. The problem is to determine $d(p)$, and a path of length $d(p)$ from s to p if $d(p) < \infty$, for all $p \in X$.

The problem can be reduced to the following instance of the optimal control problem (7). Define $U = X$, $G(s) = 0$, and $G(p) = \infty$ for all $p \in X \setminus \{s\}$, let g be such that $g(p, q, u) = w_{q,p}$ whenever $(q, p) \in A$, and let F be single-valued such that $F(p, U) = \{p\} \cup \{q \in X \mid (q, p) \in A\}$. Then there exists a static controller C for the system S in (4), with single-valued transition function, such that the closed-loop value function of (7) associated with C equals the value function V of (7); see e.g. Section VII-B. In turn, as is easily seen, a shortest path from s to p can be obtained from the unique element of $\mathcal{B}_p(C \times S)$, and $d = V$. □

III.5 Example (Reach-Avoid Problem). The problem of steering the state of the plant into a target set while avoiding obstacles appears in many applications, e.g. [35], [42]. For a formal description, let S be a plant of the form (4), and let a target set $D \subseteq X$ and an obstacle set $M \subseteq X$ be given. The controller $C \in \mathcal{F}(X, U)$ is successful for the state $p \in X$ if for every $(u, v, x) \in \mathcal{B}_p(C \times S)$ there exists some $s \in \mathbb{Z}_+$ satisfying $x(s) \in D$ and $x(t) \notin M$ for all $t \in [0; s]$. We say that p can be forced into the target set if there exists a controller that is successful for p. The problem is to determine the subset $E \subseteq X$ of states that can be forced into the target set, and a controller that is successful for all states in E.

The problem can be reduced to the following instance of the optimal control problem (7). Define $G(p) = 0$ if $p \in D \setminus M$, and otherwise $G(p) = \infty$, and define $g(p, q, u) = 0$ if $p \notin M$, and otherwise $g(p, q, u) = \infty$. Then E equals the effective domain $V^{-1}(\mathbb{R}_+)$ of the value function V of (7), and a controller C is successful for all states in E iff the closed-loop value function of (7) associated with C equals V.

The problem can be approximately solved using the results in this paper, which, for each compact subset $K \subseteq E$, yield a static controller C that is successful for all states in K. See Corollary VI.10. □

III.6 Example (Minimum Time Problem). Various practical problems require solving reach-avoid problems in minimum time, e.g. [26], [35], [43]. For a formal description, let S, D and M as in Example III.5, and define the *entry time* $T_C(p)$ *from* $p \in X$ *under feedback* $C \in \mathcal{F}(X, U)$ as the infimum of all $\tau \in \mathbb{Z}_+$ satisfying the following condition: For every $(u, v, x) \in \mathcal{B}_p(C \times S)$ there exists some $s \in [0; \tau]$ such that $x(s) \in D$ and $x(t) \notin M$ for all $t \in [0; s]$. The *entry time* $T(p)$ *from* $p \in X$ is the infimum of $T_C(p)$ over all controllers $C \in \mathcal{F}(X, U)$. The problem is to determine the value $T(p)$ for all $p \in X$, and a controller $C \in \mathcal{F}(X, U)$ satisfying $T = T_C$.

The problem can be reduced to the following instance of the optimal control problem (7). Define $G(p) = 0$ if $p \in D \setminus M$, and otherwise $G(p) = \infty$, and define $g(p, q, u) = 1$ if $p \notin M$, and otherwise $g(p, q, u) = \infty$. Then the *minimum time function* T equals the value function V of (7), and for every controller $C \in \mathcal{F}(X, U)$, T_C equals the closed-loop value function of (7) associated with C.

The problem can be approximately solved using the results in this paper, which, for each compact subset $K \subseteq X$, yield a static controller C satisfying $\sup T_C(K) = \sup T(K)$. See Corollary VI.10. □

IV. Fixed-point characterization and regularity of the value function

In this section, we shall first characterize the value function (9) as the maximal fixed-point of the *dynamic programming*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2018.2863178, IEEE Transactions on Automatic Control

operator P associated with the optimal control problem (7),

$$P(W)(p) = \min\left\{G(p), \inf_{u\in U} \sup_{q\in F(p,u)} g(p,q,u) + W(q)\right\}, \tag{11}$$

which maps the space of functions $X \to [0,\infty]$ into itself. This characterization will in turn permit us to represent the value function as the limit of repeated applications of P to the terminal cost function and to prove that this limit is semi-continuous. These results are new, see our discussion at the end of this section. Moreover, they will be useful later, when they facilitate the comparison of value functions in Section V as well as our convergence proofs in Section VI. In addition, as a side product we obtain the identity (10), which shows that in our setting, the value function could equivalently be defined using alternative information patterns, e.g. [28].

IV.1 Theorem. Let (7) be an optimal control problem, and let V and P be the associated value function and dynamic programming operator as defined in (9) and (11), respectively. Then V is the maximal fixed point of P, i.e., $P(V) = V$, and $W \leq P(W)$ implies $W \leq V$. Moreover, the identity (10) holds for all $p \in X$. □

Proof. We first observe that P is monotone, i.e., that $P(W) \leq P(W')$ whenever $W \leq W'$, and that

$$J(u,v,x) = G(x(0)) \qquad \text{if } v(0) = 1,$$
$$J(u,v,x) = g(x(0),x(1),u(0)) + J(\sigma u,\sigma v,\sigma x), \text{ otherwise,}$$

for all $(u,v,x) \in (U \times \{0,1\} \times X)^{\mathbb{Z}_+}$. Using a controller whose transition function maps into $Z \times U \times \{1\}$, for some Z, we see that $V \leq G$.

In what follows, we shall denote by $R(p)$ the right hand side of (10) to show that $R \leq V \leq P(V)$ and that $W \leq P(W)$ implies $W \leq R$, which proves the theorem. In particular, the case $W = P(V)$ shows that $P(V) \leq V$.

To prove that $R \leq V$ holds, assume that $V(p) < R(p)$ for some $p \in X$. Then there exists a controller C of the form (5) and a map $\beta \in \Delta(p)$ satisfying $J(u,v,x) < J(u,v,\beta(u))$ for every $(u,v,x) \in \mathcal{B}_p(C \times S)$, where S denotes the system (4). We will inductively construct u and v such that $(u,v,\beta(u)) \in \mathcal{B}_p(C \times S)$, which is a contradiction and so proves $R \leq V$. To this end, consider the following condition for any $T \in \mathbb{Z}_+$: The signals u and v have already been defined on $[0;T[$, and the signal z has already been defined on $[0;T]$ such that (3) with $\beta(u)$ in place of x holds for all $t \in [0;T[$. Here, $\beta(u)(t)$ denotes $\beta(\tilde{u})(t)$ for any extension $\tilde{u}\colon \mathbb{Z}_+ \to U$ of u, which is an unambiguous abbreviation as β is causal. Pick any $z(0) \in Z_0$ to satisfy the condition for $T = 0$, and assume the condition holds for some $T \in \mathbb{Z}_+$. To extend the signals u, v, and z we pick $(z(T+1),u(T),v(T)) \in H(z(T),\beta(u)(T))$, which is feasible as β is strictly causal. Then the condition holds with $T+1$ in place of T as β is causal. Consequently, there exist signals u, v and z defined on $\mathbb{Z}_+$ such that $(u,v,z,\beta(u))$ is a solution of C, and so $(u,v,\beta(u)) \in \mathcal{B}_p(C \times S)$ as $\beta \in \Delta(p)$.

To prove that $V \leq P(V)$ holds, it suffices to show that

$$V(p) \leq \sup_{q\in F(p,\xi)} g(p,q,\xi) + V(q) \tag{12}$$

for all $p \in X$ and all $\xi \in U$. To this end, let $p \in X$, $\xi \in U$ and $\varepsilon > 0$. For every $q \in F(p,\xi)$ there is a controller $C_q \in \mathcal{F}(X,U)$ such that

$$\sup_{(u,v,x)\in\mathcal{B}_q(C_q\times S)} J(u,v,x) \leq V(q) + \varepsilon. \tag{13}$$

We may assume without loss of generality that C_q is of the form $C_q = (Z_q, \{z_{q,0}\}, X, U, H_q)$, in which the state alphabets Z_q are pairwise disjoint. Let $z_0, z_1 \notin Z_q$ for every q, $z_0 \neq z_1$, define $Z = \{z_0, z_1\} \cup \bigcup_{q\in F(p,\xi)} Z_q$, and let μ be a controller for S of the form $(Z, \{z_0\}, X, U, H)$ that satisfies the following conditions for every $q \in F(p,\xi)$: $H(z_0,p) = \{(z_1,\xi,0)\}$, $H(z_1,q) = H_q(z_{q,0},q)$, and $H(z,\cdot) = H_q(z,\cdot)$ whenever $z \in Z_q$. One easily shows that $(u,v,x) \in \mathcal{B}_p(\mu \times S)$ implies $x(0) = p$, $v(0) = 0$, $u(0) = \xi$, $x(1) \in F(p,\xi)$, and $(\sigma u,\sigma v,\sigma x) \in \mathcal{B}_{x(1)}(C_{x(1)} \times S)$. Using the definition of V, the observation at the beginning of this proof, and (13), it then follows that $V(p) \leq \sup_{q\in F(p,\xi)} g(p,q,\xi) + V(q) + \varepsilon$. This implies (12), and so $V \leq P(V)$.

Finally, suppose that $W \leq P(W)$ and that $R(p) + 2\varepsilon < W(p)$ for some $p \in X$ and some $\varepsilon > 0$. We claim that there exists a map $\beta \in \Delta(p)$ such that

$$R(p) + (1 + 2^{-t})\varepsilon < W(\beta(u)(t)) + \Sigma(\beta(u),u,t) \tag{14}$$

holds for all $t \in \mathbb{Z}_+$ and all $u\colon \mathbb{Z}_+ \to U$, where Σ is defined by $\Sigma(x,u,t) = \sum_{\tau=0}^{t-1} g(x(\tau),x(\tau+1),u(\tau))$. Since $W \leq P(W) \leq G$ it then follows that $R(p) + \varepsilon \leq J(u,v,\beta(u))$ for all u and v, which contradicts the definition of R, and hence, shows that $W \leq P(W)$ implies $W \leq R$.

To prove our claim, we define $\beta(u)(0) = p$ for every u, so that the inequality (14) for $t = 0$ reduces to our assumption on ε. Next, we assume that for some $t \in \mathbb{Z}_+$ and all $\tau \in [0;t]$, the value of $\beta(u)|_{[0;\tau]}$ has already been defined as a function of $u|_{[0;\tau[}$ such that (14) holds. Then the inequality $W \leq P(W)$ implies that given $u|_{[0;t+1[}$, there is some $q \in F(\beta(u)(t),u(t))$ such that $W(\beta(u)(t)) \leq 2^{-(t+1)}\varepsilon + g(\beta(u)(t),q,u(t)) + W(q)$. Hence, the choice $\beta(u)(t+1) = q$ defines $\beta(u)|_{[0;t+1]}$ as a function of $u|_{[0;t+1[}$ such that (14) holds with $t+1$ in place of t. This proves our claim, and completes the proof. □

For our representation of the value function as the semi-continuous limit of value iteration, i.e., of successive applications of the dynamic programming operator P to the terminal cost function G, we consider the following hypothesis.

($\mathrm{A_1}$) X and U are metric spaces, F is compact-valued, and g, G and F are u.s.c..

IV.2 Corollary. In the setting of Theorem IV.1, additionally assume ($\mathrm{A_1}$). Then V is u.s.c.,

$$V(p) = \lim_{T\to\infty} P^T(G)(p) \tag{15}$$

for all $p \in X$, and $P^{T+1}(G) \leq P^T(G)$ for all $T \in \mathbb{Z}_+$. □

Proof. Obviously, $0 \leq P(W) \leq G$ for every $W\colon X \to [0,\infty]$, and P is monotone. This proves the monotonicity claim and shows that the limit on the right hand side of (15), which we will denote by $V_\infty(p)$, exists in $[0,\infty]$. In addition, the inequality $V \leq G$ implies $V \leq P^T(G)$ for all $T \in \mathbb{Z}_+$,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2018.2863178, IEEE Transactions on Automatic Control

hence $V \leq V_\infty$. Next, using Berge's Maximum Theorem A.2 and the fact that the infimum of u.s.c. maps is u.s.c., we see that $P(W)$ is u.s.c. if W is. Thus, $P^T(G)$ is u.s.c. for every $T \in \mathbb{Z}_+$. Then V_∞ is u.s.c. as it is the infimum of u.s.c. maps.

It remains to show that $V_\infty \leq P(V_\infty)$. Then Theorem IV.1 implies that $V_\infty \leq V$, and so $V_\infty = V$. Indeed, as $P^T(G)$ is monotonically decreasing in T, we may apply Proposition A.3 with $f_k(q) := g(p,q,u) + P^k(G)(q)$ to see that

$$\lim_{T\to\infty} \sup_q g(p,q,u) + P^T(G)(q) = \sup_q g(p,q,u) + V_\infty(q)$$

for arbitrary p and u, where the suprema are over $q \in F(p,u)$. As the limit is an infimum, we have $\lim_{T\to\infty} P(P^T(G))(p) = P(V_\infty)(p)$, which completes the proof. □

We note that while Theorem IV.1 does not assume any regularity of the problem data, the hypothesis (A_1) mandates that e.g. in the Reach-Avoid Problem of Example III.5 the target set and the obstacle set is open and closed, respectively. Moreover, if any one of the assumptions in (A_1) is dropped, then the identity (15) fails to hold, in general. Also our assumptions of semi-continuity and compact-valuedness in (A_1) are automatically satisfied if the state and input alphabets are finite.

We would like to emphasize that while fixed-point characterizations and value iteration methods are well known in the field of Dynamic Programming, e.g. [4], [12], [13], [44], [45], the available results do not apply in our setting. Specifically, the theory in [12] requires that cost functionals are represented as limits of finite horizon costs, which is impossible for the functional in (6). The hypotheses in [44] imply that the dynamic programming operator has a unique fixed-point, and so are not satisfied by e.g. the Reach-Avoid Problem of Example III.5 whenever the transition function F is single-valued and there exists a state that cannot be forced into the target set. Similarly, for the unconstrained Minimum Time Problem of Example III.6, the hypotheses in [13] imply that the entry time is finite for every state [13, Sect. 3.2.1], or alternatively, that there exists a uniform bound on all finite entry times [13, Sect. 3.2.2]. These assumptions are typically not satisfied if the state alphabet of the plant is infinite, and are not imposed in the present paper. Results on stochastic games, e.g. [4], [45], can be directly interpreted in our setting only if the transition function of the plant is single-valued. In addition, running costs are typically assumed to vanish and terminal costs are required to be real-valued. Moreover, the class of controllers is also restricted, which can be seen from the result [45, Ch. 2.9, Th. 1] which does not hold in our setting: If the state alphabet of the plant is finite and the controller eventually stops every solution of the closed-loop, then the stopping times are uniformly bounded.

V. Comparison of Closed-Loop Performances

In this section, we introduce *valuated alternating simulation relations* and *valuated feedback refinement relations* between optimal control problems, which are novel, quantitative variants of known qualitative system relations. As we shall show, the former concept allows for the efficient comparison of value functions of related optimal control problems, while the latter guarantees that the concrete closed-loop value function is upper-bounded, in a well-defined sense, by the abstract closed-loop value function. These results will be needed in the proofs of our main results in Section VI.

A. Comparison of value functions

V.1 Definition. Consider optimal control problems

$$\Pi_i = (X_i, U_i, F_i, G_i, g_i), \tag{16}$$

and denote the dynamic programming operator associated with the problem Π_i by P_i, $i \in \{1,2\}$. The relation $Q \colon X_1 \rightrightarrows X_2$ is a *valuated alternating simulation relation* from Π_1 to Π_2, denoted by $\Pi_1 \preccurlyeq_Q^\circ \Pi_2$, if the following conditions hold for all $(p_1,p_2) \in Q$ and all $u_2 \in U_2$:

(i) $G_1(p_1) \leq G_2(p_2)$;

(ii) if $G_1(p_1) > 0$ and the maps $g_2(p_2,\cdot,u_2)$ and $(P_1(0)) \circ Q^{-1}$ are bounded on the set $F_2(p_2,u_2)$, where 0 denotes the zero function on X_1, then for all $\varepsilon > 0$ we have:

$$\begin{aligned}&\exists_{u_1\in U_1} \forall_{q_1\in F_1(p_1,u_1)} \exists_{q_2 \in F_2(p_2,u_2)\cap Q(q_1)} \\ &\qquad g_1(p_1,q_1,u_1) \leq \varepsilon + g_2(p_2,q_2,u_2).\end{aligned} \tag{17}$$

□

The notion of valuated alternating simulation relation is related to its well-known qualitative variant in [1] as well as to the quantitative variants employed in [5], [7], [10]. The concepts in [1], [5], [7], [10] require that the first line of condition (17) holds for all $(p_1,p_2) \in Q$ and all $u_2 \in U_2$, which implies, roughly speaking, behavioral inclusion between the two dynamical systems underlying the optimal control problems Π_1 and Π_2. It is the weaker conditions imposed in Definition V.1 that facilitate the application of valuated alternating simulation relations in our convergence proof in Section VI-B, where behavioral inclusion cannot be presumed. Comparison of the value functions associated with two related optimal control problems is still possible using our fixed-point characterization in Theorem IV.1:

V.2 Theorem. Let Π_1 and Π_2 be two optimal control problems with value functions V_1 and V_2, respectively. If $\Pi_1 \preccurlyeq_Q^\circ \Pi_2$, then $V_1(p_1) \leq V_2(p_2)$ for every $(p_1,p_2) \in Q$. □

Proof. Suppose that Π_i is of the form (16) and let P_i be the associated dynamic programming operator, $i \in \{1,2\}$. We claim that $P_1(V_1)(p_1) \leq P_2(W)(p_2)$ for all $(p_1,p_2) \in Q$, where the function $W \colon X_2 \to [0,\infty]$ is defined by

$$W(p_2) = \sup\{V_1(p_1) \mid (p_1,p_2) \in Q\}. \tag{18}$$

Then, by applying Theorem IV.1 twice, we obtain $W \leq P_2(W)$, and in turn, $W \leq V_2$, which proves the assertion.

Let $(p_1,p_2) \in Q$. Our claim is obvious if $G_1(p_1) = 0$, so we may assume throughout that $G_1(p_1) > 0$. Moreover, from Definition V.1(i), we see that it suffices to prove that

$$\begin{aligned}&\inf_{u_1\in U_1} \sup_{q_1\in F_1(p_1,u_1)} g_1(p_1,q_1,u_1) + V_1(q_1) \\ &\qquad\qquad \leq \sup_{q_2\in F_2(p_2,u_2)} g_2(p_2,q_2,u_2) + W(q_2)\end{aligned} \tag{19}$$

holds for all $u_2 \in U_2$.

Let $u_2 \in U_2$, denote the value of the right hand side of (19) by R, and suppose that $R < \infty$. Then the map $g_2(p_2, \cdot, u_2)$ is bounded on the set $F_2(p_2, u_2)$. The same holds for the map $(P_1(0)) \circ Q^{-1}$ as $V_1 = P_1(V_1) \geq P_1(0)$. Thus, we may assume that (17) holds. Moreover, the estimate (19) holds if for all $\varepsilon > 0$ there exists $u_1 \in U_1$ such that $\sup_{q_1 \in F_1(p_1,u_1)} g_1(p_1, q_1, u_1) + V_1(q_1) \leq \varepsilon + R$. This, in turn, is guaranteed if for all $q_1 \in F_1(p_1, u_1)$ there exists $q_2 \in F_2(p_2, u_2)$ satisfying $g_1(p_1, q_1, u_1) + V_1(q_1) \leq \varepsilon + g_2(p_2, q_2, u_2) + W(q_2)$, and so an application of (17) and (18) completes the proof. □

B. Controller refinement and comparison of closed-loop value functions

We have just seen that the existence of a valuated alternating simulation relation between optimal control problems implies a comparison between the respective value functions. We now proceed to introduce the stronger notion of valuated feedback refinement relation to additionally facilitate the refinement of solutions of one of the two problems, to the other problem, which is needed in the proof of one of our main results in Section VI.

V.3 Definition. Consider two optimal control problems Π_1 and Π_2 of the form (16). The relation $Q\colon X_1 \rightrightarrows X_2$ is a *valuated feedback refinement relation* from Π_1 to Π_2, denoted $\Pi_1 \preccurlyeq_Q \Pi_2$, if Q is strict and the following conditions hold for all $(p_1, p_2), (q_1, q_2) \in Q$ and all $u \in U_2$:

(i) $U_2 \subseteq U_1$;
(ii) $G_1(p_1) \leq G_2(p_2)$;
(iii) $g_1(p_1, q_1, u) \leq g_2(p_2, q_2, u)$;
(iv) $Q(F_1(p_1, u)) \subseteq F_2(p_2, u)$. □

We first note that every valuated feedback refinement relation is also a valuated alternating simulation relation. We state this simple fact as a formal result for later reference:

V.4 Proposition. $\Pi_1 \preccurlyeq_Q \Pi_2$ implies $\Pi_1 \preccurlyeq^{\circ}_Q \Pi_2$. □

Apart from conditions (ii) and (iii) in Definition V.3, and in the special case of strict transition functions considered in the present paper, the notion of valuated feedback refinement relation coincides with its qualitative variant introduced in [2]. Hence, we can take advantage of the controller refinement scheme presented in [2]. That is, we refine any abstract controller by serially connecting it with a valuated feedback refinement relation used as an interface; see Fig. 2. We therefore need to formalize the concept of serial composition:

V.5 Definition. Let C be a controller of the form (5), X' be a non-empty set and $Q\colon X' \rightrightarrows \widetilde{X}$ be a strict map. The *serial composition of Q and C*, denoted $C \circ Q$, is the controller $(Z, Z_0, X', \widetilde{U}, H')$ with $H'(z, x') = H(z, Q(x'))$. □

As demonstrated in [2] the proposed controller refinement scheme implies a comparison between closed-loop behaviors. Here we extend that result to guarantee a comparison between closed-loop value functions:

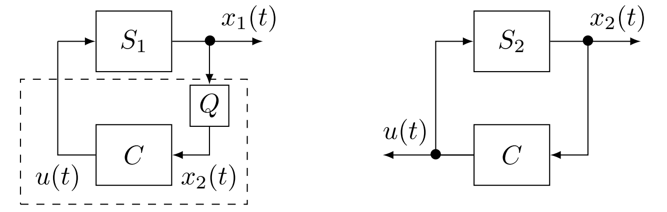

Figure 2. Using a valuated feedback refinement relation Q from S_1 to S_2, an abstract controller C is refined into the serial composition of Q and C.

V.6 Theorem. Let Π_1 and Π_2 be optimal control problems of the form (16), and suppose that $\Pi_1 \preccurlyeq_Q \Pi_2$ and $C \in \mathcal{F}(X_2, U_2)$. Then $C \circ Q \in \mathcal{F}(X_1, U_1)$ and we have

$$\forall_{p_1 \in X_1} L_1(p_1) \leq \sup L_2(Q(p_1)), \tag{20}$$

where L_1 and L_2 are the closed-loop value functions of Π_1 and Π_2 associated with $C \circ Q$ and C, respectively. □

Proof. The fact that $C \circ Q \in \mathcal{F}(X_1, U_1)$ is obvious. Denote the cost functional associated with Π_i by J_i, set $S_i = (X_i, U_i, F_i)$, $i \in \{1, 2\}$, and let $(u, v, x_1) \in \mathcal{B}((C \circ Q) \times S_1)$. We claim that there exists a signal $x_2\colon \mathbb{Z}_+ \to X_2$ satisfying $x_2(0) \in Q(x_1(0))$, $(u, v, x_2) \in \mathcal{B}(C \times S_2)$, and $J_1(u, v, x_1) \leq J_2(u, v, x_2)$. This implies (20) and completes our proof.

To prove our claim, we first note that there exists a signal z defined on $\mathbb{Z}_+$ such that (u, v, z, x_1) is a solution of $C \circ Q$ and (u, x_1) is a solution of S_1. By the former fact and Definitions III.1 and V.5, there exists a signal $x_2\colon \mathbb{Z}_+ \to X_2$ such that (u, v, z, x_2) is a solution of C and $(x_1(t), x_2(t)) \in Q$ for all $t \in \mathbb{Z}_+$. Using (iv) in Definition V.3 we obtain $x_2(t+1) \in Q(x_1(t+1)) \subseteq Q(F_1(x_1(t), u(t))) \subseteq F_2(x_2(t), u(t))$ for all t. Hence, (u, x_2) is a solution of S_2, and so $(u, v, x_2) \in \mathcal{B}(C \times S_2)$. We obviously have $J_1(u, v, x_1) \leq J_2(u, v, x_2)$ if $v = 0$, and if $v \neq 0$ the same estimate follows from (ii) and (iii) in Definition V.3. □

For easier reference in later sections, we reformulate Theorem V.6 in terms of pointwise upper performance bounds:

V.7 Definition. Let $Q\colon X_1 \rightrightarrows X_2$ be strict and let $f\colon X_2 \to [0, \infty]$. Then the function $\hat{f}^{(Q)}\colon X_1 \to [0, \infty]$ defined by

$$\hat{f}^{(Q)}(x) = \sup f(Q(x))$$

is called *pointwise upper bound of f associated with Q*. □

V.8 Corollary. Under the hypotheses and in the notation of Theorem V.6 we have $L_1 \leq \hat{L}_2^{(Q)}$. □

VI. Main results

In this section, we introduce a notion of abstraction of optimal control problems which comes with a non-negative conservatism parameter. We will then show that the concrete value function can be approximated arbitrarily closely using value functions of sufficiently precise abstractions. Moreover, we shall show that if abstract controllers can be chosen to be optimal, the performance of the closed-loop in Fig. 2 converges to the concrete value function as well. The latter result implies a kind of completeness property of controller synthesis based on abstractions of conservatism introduced in this paper, an aspect to be discussed at the end of the section.

A. Abstractions and their conservatism

To begin with, we first introduce abstractions devoid of any notion of conservatism. In doing so, we focus on a case where the abstract state space is a cover of the concrete state space, which has turned out to be canonical in the qualitative setting [2, Sec. VII]. Here, a *cover* of a set X is a set of subsets of X whose union equals X.

VI.1 Definition. Let Π_1 and Π_2 be optimal control problems of the form (16), where X_2 is a cover of X_1 by non-empty subsets. Then Π_2 is an *abstraction* of Π_1 if $\Pi_1 \preccurlyeq_{\in} \Pi_2$, where $\in\colon X_1 \rightrightarrows X_2$ denotes the membership relation. □

For later reference, we explicitly state our requirements on abstractions.

VI.2 Proposition. Let Π_1 and Π_2 be optimal control problems of the form (16), where X_2 is a cover of X_1 by non-empty subsets. Then $\Pi_1 \preccurlyeq_{\in} \Pi_2$ iff the following conditions hold whenever $p \in \Omega \in X_2$, $p' \in \Omega' \in X_2$ and $u \in U_2$:

(i) $U_2 \subseteq U_1$;
(ii) $G_1(p) \leq G_2(\Omega)$;
(iii) $g_1(p, p', u) \leq g_2(\Omega, \Omega', u)$;
(iv) $\Omega' \cap F_1(\Omega, u) \neq \varnothing \Rightarrow \Omega' \in F_2(\Omega, u)$. □

Proof. Obviously, the relation $\in$ is strict as X_2 is a cover of X_1, and if $Q = \in$, then the conditions (i) through (iii) are equivalent to the respective conditions in Definition V.3. The equivalence of condition (iv) to the condition (iv) in Definition V.3 is obtained by an application of [2, Prop. VII.1] to the systems $S_i = (X_i, X_i, U_i, U_i, X_i, F_i, \mathrm{id})$, $i \in \{1, 2\}$. □

As we can see, even rather conservative approximations of the concrete optimal control problem may qualify as abstractions. We aim at resolving that issue by introducing a suitable notion of *conservatism*. To this end, we first need to introduce some additional notation. For any metric space (X, d) we define

$$d(x, N) = \inf \{d(x, y) \,|\, y \in N\},$$
$$d(M, N) = \inf \{d(x, y) \,|\, x \in M, y \in N\}$$

for all $x \in X$ and all nonempty subsets $M, N \subseteq X$. We use $B(c, r)$ and $\bar{B}(c, r)$ to denote the open, respectively, closed ball with center $c \in X$ and radius $r > 0$, and we adopt the convention that $\bar{B}(c, 0) = \{c\}$. We denote the diameter of a subset $M \subseteq X$ by $\mathrm{diam}(M)$. See [34].

VI.3 Definition. Let Π_2 be an abstraction of Π_1 and suppose that Π_1 and Π_2 are of the form (16), that U_1 and X_1 are metric spaces, and that the elements of X_2 are closed subsets of X_1. Then Π_2 is an *abstraction of conservatism* ∞ of Π_1. Moreover, Π_2 is an *abstraction of conservatism* $\rho \in \mathbb{R}_+$ of Π_1 if the following conditions hold for all $\Omega, \Omega' \in X_2$ and all $u \in U_2$:

(i) $U_1 = \bar{B}(U_2, \rho)$;
(ii) $G_2(\Omega) \leq \rho + \sup G_1(\Omega)$;
(iii) $g_2(\Omega, \Omega', u) \leq \rho + \sup g_1(\Omega, \Omega', u)$.

If Ω satisfies the condition

$$G_1(\Omega) \cup g_1(\Omega, X_1, U_1) \neq \{\infty\}, \tag{21}$$

then we additionally require the following:

(iv) $F_2(\Omega, u) \subseteq \{\Omega'' \in X_2 \,|\, d(\Omega'', F_1(\Omega, u)) \leq \rho\}$, where d denotes the metric on X_1;
(v) $\mathrm{diam}(\Omega) \leq \rho$. □

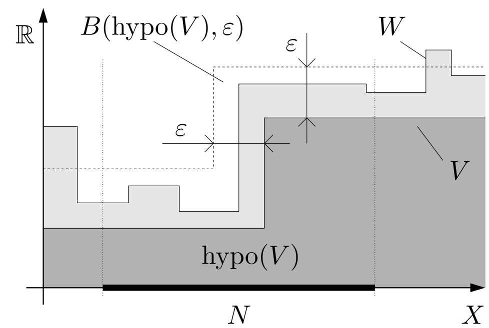

Figure 3. Approximation of the hypograph of the map $V\colon X \to \mathbb{R}_+ \cup \{\infty\}$ by the hypograph of $W \geq V$, on the subset $N \subseteq X$ [46].

As we had announced, Definition VI.3 limits the conservatism of abstractions. Specifically, while the conditions (i) through (iv) in Proposition VI.2 demand that U_1, $G_2(\Omega)$, $g_2(\Omega, \Omega', u)$ and $F_2(\Omega, u)$ merely over-approximate U_2, $\sup G_1(\Omega)$, $\sup g_1(\Omega, \Omega', u)$ and $F_1(\Omega, u)$, respectively, the respective conditions in Definition VI.3 mandate that the approximation error does not exceed the value of the conservatism parameter ρ, and (v) bounds the error by which abstract states over-approximate concrete states. The condition (21) restricts the requirements (iv) and (v) to regions where the concrete value function is possibly finite.

B. Arbitrarily close approximation of concrete value functions

We next need to choose a suitable notion of convergence. On the one hand, pointwise convergence is not powerful enough, e.g. to imply our completeness results in Section VI-C, and similarly for convergence in Lebesgue spaces as employed in [28]. On the other hand, the stronger concept of uniform convergence would require that any points of discontinuity of the concrete value function are also present, exactly and not only approximately, in the functions to approximate it, which is not realistic to assume. We here rely on a concept that lies in between the aforementioned extremes, and the first main result of our paper shows that the hypographs of pointwise upper bounds of the abstract value functions locally approximate the hypograph of the concrete value function. See Fig. 3. The result requires tightening the hypothesis (A_1) on the optimal control problem (7) as follows:

($\mathbf{A_2}$) X is a proper metric space, U is a compact metric space, F is compact-valued, and g, G and F are u.s.c..

Here, a metric space is *proper* if every closed ball is compact, a requirement satisfied, e.g. by $\mathbb{R}^n$ and by all of its closed metric subspaces. Hypothesis (A_2) is extended to optimal

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2018.2863178, IEEE Transactions on Automatic Control

control problems Π_i of the form (16) in the obvious way. In the following, we do not mention explicitly the association of pointwise upper bounds on abstract value functions with the respective membership relations.

VI.4 Theorem. Let Π be the optimal control problem (7) and let V denote the value function of Π. Then the pointwise upper bound of the value function of any abstraction of Π is an upper bound on V. If (7) additionally satisfies (A_2), then for every $p \in X$ and every $\varepsilon > 0$ there exist a neighborhood $N \subseteq X$ of p and some $\rho \in \mathbb{R}_+ \setminus \{0\}$ such that

$$(N \times \mathbb{R}) \cap \operatorname{hypo} W \subseteq B(\operatorname{hypo} V, \varepsilon) \tag{22}$$

holds whenever W is the pointwise upper bound on the value function of an abstraction of conservatism ρ of (7). □

To prove the theorem we will introduce an auxiliary optimal control problem Π_3 with the following properties. Firstly, the state space X_3 of Π_3 comprises both a copy of the concrete state space and (almost the whole of) the state spaces of all abstractions, of arbitrary conservatism. Secondly, the value function V_3 of Π_3 restricted to the concrete state space coincides with the concrete value function V. Thirdly, V_3 is an upper bound on any abstract value function, on the respective subset of X_3. Using the semi-continuity of V_3 on the whole of X_3, we then conclude that the abstract value function arbitrarily closely approximates V whenever the abstract state space sufficiently closely approximates the concrete one.

In our proof below, the notion of *graph* of a set-valued map $f\colon X \rightrightarrows Y$ refers to the set $\{(x, y) \in X \times Y \mid y \in f(x)\}$, and we also use the space $K(X)$ of non-empty compact subsets of X endowed with the Hausdorff metric [33], [34] associated with the metric on X, and its subspaces $K_\rho(X)$ defined by

$$K_\rho(X) = \{\Omega \in K(X) \mid \operatorname{diam} \Omega \leq \rho\}.$$

VI.5 Lemma. Let Π_1 be an optimal control problem of the form (16) that satisfies (A_2), and denote the metric on X_1 by d. Let $\Pi_3 = (X_3, U_3, F_3, G_3, g_3)$ be given by $X_3 = K(X_1) \times \mathbb{R}_+$, $U_3 = U_1$ and

$$\begin{aligned} &F_3((\Omega, \rho), u) = \\ &\qquad \{\Omega' \in K_\rho(X_1) \mid d(\Omega', F_1(\Omega, \bar{B}(u, \rho))) \leq \rho\} \times \{\rho\}, \\ &G_3((\Omega, \rho)) = \rho + \sup G_1(\Omega), \\ &g_3((\Omega, \rho), (\Omega', \rho'), u) = \rho + \sup g_1(\Omega, \Omega', \bar{B}(u, \rho)). \end{aligned}$$

Then Π_3 is an optimal control problem satisfying (A_2). □

Proof. Π_3 is clearly an optimal control problem by our hypotheses, and in particular, F_3 is strict. Moreover, U_3 is compact, and $K(X_1)$ is proper as X_1 is so. In addition, using Proposition A.4 it is easily seen that the maps $\alpha\colon K(X_1) \rightrightarrows X_1$ and $\beta\colon U_1 \times \mathbb{R}_+ \rightrightarrows U_1$ given by $\alpha(\Omega) = \Omega$ and $\beta(u, r) = \bar{B}(u, r)$ are u.s.c. and compact-valued, or *usco* for short. Then G_3 and g_3 are u.s.c. by Theorem A.2.

To show that F_3 is usco, define the map $H\colon K(X_1) \times U_1 \times \mathbb{R}_+ \rightrightarrows X_1$ by $H(\Omega, u, \rho) = \beta(F_1(\alpha(\Omega), \beta(u, \rho)), \rho)$, let $(((\Omega_k, \rho_k), u_k), (\Omega'_k, \rho_k))_{k \in \mathbb{N}}$ be a sequence in the graph of F_3, and suppose that the sequences Ω, ρ and u converge to $\Gamma \in K(X_1)$, $r \in \mathbb{R}_+$ and $v \in U_1$, respectively. Then $\Omega'_k \in K_{\rho_k}(X_1)$ for all k, and since F_1 is usco, we also have $\Omega'_k \cap H(\Omega_k, u_k, \rho_k) \neq \varnothing$ for all k. Thus, there exists a sequence $(p_k)_{k \in \mathbb{N}}$ satisfying $p_k \in \Omega'_k \cap H(\Omega_k, u_k, \rho_k)$ for all k, and by Proposition A.4, a subsequence of p converges to some $q \in H(\Gamma, v, r)$ since H is usco. We may assume that the whole sequence converges. Then the sequence Ω' is bounded, and so may be assumed to converge to some $\Gamma' \in K(X_1)$ since $K(X_1)$ is proper. Additionally, $\Gamma' \in K_r(X_1)$ by the continuity of the map diam on $K(X_1)$, and $q \in \Gamma'$. We conclude that $(\Gamma', r) \in F_3((\Gamma, r), v)$, and so F_3 is usco by Prop. A.4. □

VI.6 Lemma. Under the hypotheses and in the notation of Lemma VI.5, let Π_2 be an abstraction of conservatism $\rho \in \mathbb{R}_+$ of Π_1, of the form (16). Let V_i denote the value function of Π_i, $i \in \{1, 2, 3\}$, and let $X'_2 \subseteq X_2$ be the subset of cells Ω that satisfy (21). Then the following holds:

(i) $V_1(p) = V_3(\{p\}, 0)$ for all $p \in X_1$;
(ii) $V_2(\Omega) \leq V_3(\Omega, \rho)$ for all $\Omega \in X'_2$;
(iii) $V_2(\Omega) \leq V_3(\{p\}, \rho)$ whenever $p \in \Omega \in X_2 \setminus X'_2$. □

Proof. We claim that $\Pi_1 \preccurlyeq^\circ_Q \Pi_3 \preccurlyeq^\circ_{Q^{-1}} \Pi_1$ holds for the single-valued map $Q\colon X_1 \rightrightarrows X_3$ given by $Q(p) = (\{p\}, 0)$. Indeed, let $p \in X_1$ and $u \in U_3$. Then $G_3(Q(p)) = G_1(p)$ and $g_3(Q(p), Q(q), u) = g_1(p, q, u)$ for all $q \in X_1$. Moreover, $Q(F_1(p, u)) = F_3((\{p\}, 0), u)$ as F_1 is compact-valued. Thus, both conditions in Definition V.1 are met with Π_3 in place of Π_2, and they are also met with Π_3 and Π_1 in place of Π_1 and Π_2, respectively. This proves our claim, and (i) follows from Theorem V.2.

To prove (ii) and (iii) we shall show that $\Pi_2 \preccurlyeq^\circ_Q \Pi_3$ holds for the relation $Q\colon X_2 \rightrightarrows X_3$ given by $Q(\Omega) = \{(\Omega, \rho)\}$ if $\Omega \in X'_2$, and by $Q(\Omega) = \{(\{p\}, \rho) \mid p \in \Omega\}$, otherwise.

Let $(\Omega, (\Omega', \rho)) \in Q$ and $u_3 \in U_3$. Then $\Omega' \subseteq \Omega$, and additionally $(\Omega', \rho) \in X_3$ as required since $X'_2 \subseteq K_\rho(X_1)$. Moreover, the estimate $G_2(\Omega) \leq G_3(\Omega', \rho)$ is immediate from Definition VI.3 if $\Omega \in X'_2$. It also holds if $\Omega \in X_2 \setminus X'_2$, for then (21) is violated, which implies $G_3(\Omega', \rho) = \infty$. Hence, the first requirement in Definition V.1 is met with Π_2 and Π_3 in place of Π_1 and Π_2, respectively.

In our proof of the second requirement we may assume that the map $g_3((\Omega', \rho), \cdot, u_3)$ is bounded on the set $F_3((\Omega', \rho), u_3)$. Then $g_1(\Omega', X_1, u_3) \neq \{\infty\}$ by the definition of g_3, and so $\Omega = \Omega' \in X'_2$. We next pick any $u_2 \in \bar{B}(u_3, \rho) \cap U_2$, which is possible by condition (i) in Definition VI.3, and any $\Omega'' \in F_2(\Omega, u_2)$. Then the condition (iv) in Def. VI.3 shows that

$$d(\Omega'', F_1(\Omega, \bar{B}(u_3, \rho))) \leq \rho. \tag{23}$$

If $\Omega'' \in X'_2$, then $(\Omega'', \rho) \in F_3((\Omega, \rho), u_3) \cap Q(\Omega'')$. Moreover, the condition (iii) in Definition VI.3 with Ω'' and u_2 in place of Ω' and u, respectively, shows that $g_2(\Omega, \Omega'', u_2) \leq g_3((\Omega, \rho), (\Omega'', \rho), u_3)$, and we are done. If, on the other hand, $\Omega'' \notin X'_2$, then $G_1(\Omega'') \cup g_1(\Omega'', X_1, U_1) = \{\infty\}$, and hence, $G_2(\Omega'') = \infty$ and $g_2(\Omega'', X_2, U_2) = \{\infty\}$ by Proposition VI.2. This shows that $(P_2(0))(\Omega'') = \infty$. Moreover, $(\{q\}, \rho) \in F_3((\Omega, \rho), u_3)$ for some $q \in \Omega''$ by (23) and a compactness argument. Since additionally $(\{q\}, \rho) \in Q(\Omega'')$ it follows that the map $(P_2(0)) \circ Q^{-1}$ is not bounded on the set $F_3((\Omega, \rho), u_3)$, which completes our proof. □

Proof of Theorem VI.4. The first claim of the theorem directly follows from Def. VI.1, Prop. V.4, and Th. V.2. To prove the second claim, let $\varepsilon > 0$, $p \in X$ and $\rho > 0$, let Π_i, V_i and X_2' be as in Lemmas VI.5 and VI.6, $i \in \{1, 2, 3\}$, let $N = B(p, \varepsilon) \subseteq X_1$, and let W be the pointwise upper bound of V_2. If (22) does not hold with V_1 in place of V, then there exists $x \in N$ satisfying $V_1(p) + \varepsilon/2 < W(x)$. Then $V_1(p) + \varepsilon/2 < V_2(\Omega')$ for some $\Omega' \in X_2$ containing x, by the definition of W, and $V_2(\Omega') \leq V_3(\Omega, \rho)$ for some $\Omega \in K_\rho(X_1)$ containing x, by Lemma VI.6; specifically, $\Omega = \Omega'$ if $\Omega' \in X_2'$, and $\Omega = \{x\}$, otherwise.

We conclude that, if the second claim of the theorem does not hold, then there exist $\varepsilon > 0$, $p \in X$ and a sequence $(\Omega_k)_{k\in\mathbb{N}}$ in $K(X_1)$ converging to $\{p\}$ such that $V_1(p)+\varepsilon/2 < V_3(\Omega_k, 1/k)$ for all $k \in \mathbb{N}$. On the other hand, V_3 is u.s.c. by Lemma VI.5 and Corollary IV.2, and this together with Lemma VI.6(i) shows that $\limsup_{k\to\infty} V_3(\Omega_k, 1/k) \leq V_1(p)$, which is a contradiction. $\square$

C. Convergence of the closed-loop performance to the concrete value function

Finally, we will demonstrate that the performance of the concrete closed-loop in Fig. 2 converges to the concrete value function, in which we use the following notion of convergence; see [33], [34] and Proposition A.1 in the Appendix.

VI.7 Definition. Let the map $V\colon X \to \mathbb{R}_+ \cup \{\infty\}$ be u.s.c. on the metric space X, and let $L_i\colon X \to \mathbb{R}_+ \cup \{\infty\}$ satisfy $L_i \geq V$, for all $i \in \mathbb{N}$. Then the sequence $(L_i)_{i\in\mathbb{N}}$ *hypo-converges* to V, denoted $V = \text{h-lim}_{i\to\infty} L_i$, if the following condition holds. For every $p \in X$ and every $\varepsilon > 0$ there exist a neighborhood $N \subseteq X$ of p such that the inclusion

$$(N \times \mathbb{R}) \cap \operatorname{hypo} L_i \subseteq B(\operatorname{hypo} V, \varepsilon) \tag{24}$$

holds for all sufficiently large $i \in \mathbb{N}$. $\square$

In addition to hypothesis (A_2), throughout the rest of this section we shall assume the following.

($\mathbf{A_3}$) (i) For every $i \in \mathbb{N}$, Π_i is an abstraction of conservatism $\rho_i \in \mathbb{R}_+ \cup \{\infty\}$ of (7), of the form (16), C_i is an optimal controller for Π_i, and L_i is the closed-loop value function of (7) associated with $C_i \circ \in$, where $\in\colon X \rightrightarrows X_i$ is the membership relation and $\lim_{i\to\infty} \rho_i = 0$.
(ii) V is the value function of (7).

Here, $C_i \in \mathcal{F}(X_i, U_i)$ is an *optimal controller* for Π_i if the value function of Π_i coincides with the closed-loop value function of Π_i associated with C_i, i.e., if C_i realizes the achievable performance of the abstract closed-loop. As detailed in Section VII, optimal abstract controllers exist whenever abstractions are finite, and finite, arbitrarily precise abstractions can actually be computed in the case of sampled-data control system dynamics.

We are now ready to present our second main result.

VI.8 Theorem. Assume (A_2), (A_3). Then $\underset{i\to\infty}{\text{h-lim}}\, L_i = V$. $\square$

Proof. Obviously, $L_i \geq V$ for all i, X is a metric space, and V is u.s.c. by Corollary IV.2. Let W_i be the value function of Π_i, and let $p \in X$ and $\varepsilon > 0$. By Theorem VI.4 there exists a neighborhood $N \subseteq X$ of p such that $(N \times \mathbb{R}) \cap \operatorname{hypo} \hat{W}_i^{(\in)} \subseteq B(\operatorname{hypo} V, \varepsilon)$ holds for all sufficiently large $i \in \mathbb{N}$. Then, since $L_i \leq \hat{W}_i^{(\in)}$ for all i by Corollary V.8, the requirement in Definition VI.7 is satisfied. $\square$

The theorem implies that the concrete value function V is uniformly approximated on compact sets by the actual closed-loop performances L_i. Specifically, for every $\varepsilon > 0$ and every compact subset $N \subseteq X$ the inclusion (24) holds for all sufficiently large $i \in \mathbb{N}$. See also Fig. 3. Theorem VI.8 also implies pointwise convergence, and it even implies uniform convergence on any set on which such a strong convergence property can possibly be expected:

VI.9 Corollary. Assume (A_2) and (A_3). Then we have

$$V(p) = \lim_{i\to\infty} L_i(p) \quad \text{for all } p \in X, \tag{25}$$

and the following holds for every compact subset $N \subseteq X$.

(i) For every $\varepsilon > 0$ and all sufficiently large $i \in \mathbb{N}$ we have $\sup L_i(N) \leq \varepsilon + \sup V(N)$.
(ii) If V is real-valued on N, then $\sup V(N) < \infty$, and if V is additionally continuous on N, then the convergence in (25) is uniform with respect to $p \in N$. $\square$

Proof. If (i) does not hold, then there exist $\varepsilon > 0$, $p \in N$ and a sequence $(x_i)_{i\in\mathbb{N}}$ in N converging to p and satisfying $L_i(x_i) > \varepsilon+\sup V(N)$ for infinitely many $i \in \mathbb{N}$. This implies $\limsup_{i\to\infty} L_i(x_i) > V(p)$, which contradicts Proposition A.1. The same argument with the inequality $L_i(x_i) > \varepsilon + V(x_i)$ proves the second claim in (ii), and the first claim follows since V is u.s.c. by Corollary IV.2, and so $V(N) \subseteq \mathbb{R}$ implies $\sup V(N) < \infty$. Finally, the identity (25) follows from the estimate $V \leq L_i$ and the special case $N = \{p\}$ of (i). $\square$

An interesting special case arises when the cost functions (2) map into the discrete set

$$D = \lambda\mathbb{Z}_+ \cup \{\infty\} \tag{26}$$

for some $\lambda \in \mathbb{R}_+$, in which the subcase $\lambda = 0$, or equivalently, $D = \{0, \infty\}$, corresponds to qualitative problems. Then, without loss of generality, all abstract cost functions map into the set (26) either. We would like to explicitly spell out this case, which includes, e.g. the Reach-Avoid Problem and the Minimum Time Problem in Examples III.5 and III.6:

VI.10 Corollary. Assume (A_2) and (A_3). Suppose that both the concrete cost functions g and G and the abstract cost functions g_i and G_i map into the set (26), for some $\lambda \in \mathbb{R}_+$ and every $i \in \mathbb{N}$.
Then for every compact subset $N \subseteq X$ we have $\sup L_i(N) = \sup V(N)$ for all sufficiently large $i \in \mathbb{N}$. In particular, if $\lambda = 0$ and V vanishes on some compact subset $N \subseteq X$, so does L_i for all sufficiently large $i \in \mathbb{N}$. $\square$

Assertion (i) in Corollary VI.9 and Corollary VI.10 can be seen as a completeness results. Indeed, if for every initial state in a compact subset $N \subseteq X$ the achievable closed-loop performance for (7) is finite, then using sufficiently precise abstractions it is possible to synthesize controllers for (7) whose worst-case performance gaps on N are arbitrarily small. In particular, we obtain controllers to solve qualitative problems on the whole of N whenever such controllers exist. This is in contrast with somewhat related results from the literature. Specifically, there is a method that, given a qualitative control problem and some perturbation of that problem, returns either a solution to the former problem in the form of a controller, or a proof that the latter problem is not solvable [47, Cor. 2]. Analogous results for verification problems appear in [48]. While the method does apply to arbitrarily small perturbations, it is not guaranteed, by the theory in [47], to ever return a controller even if the original, unperturbed problem is solvable.

VII. Algorithmic Solution

The practical applicability of our main results in Section VI depends on our ability to both compute finite abstractions of arbitrary conservatism and solve finite optimal control problems. For the sake of self-consistency of the present paper, we shall discuss both issues, where for the former problem we focus on our solution in [31] for a class of optimal control problems arising in the context of sampled-data control systems. Using e.g. the method from [49, Sec. 8.2], it is straightforward to adapt our solution to the simpler case where the transition function of the plant is given explicitly, rather than implicitly through sampling a continuous-time system.

A. A sampled optimal control problem

We introduce a class of optimal control problems for which we devised an algorithm in [31] to compute finite abstractions of arbitrary conservatism. The discrete-time plant represents the sampled behavior of a continuous-time control system, which we describe by a nonlinear differential equation with additive, bounded disturbances of the form

$$\dot{x} \in f(x,u) + [\![-w,w]\!] \tag{27}$$

where $f\colon \mathbb{R}^n \times U \to \mathbb{R}^n$, $U \subseteq \mathbb{R}^m$, and $w \in \mathbb{R}^n_+$. Here, the summation in (27) is interpreted as the Minkowski set addition [33], and $[\![-w,w]\!]$ denotes a *hyper interval* in $\mathbb{R}^n$ given by $[\![-w,w]\!] = [-w_1,w_1] \times \ldots \times [-w_n,w_n]$. Given an input signal $u\colon J \subseteq \mathbb{R} \to U$, a locally absolutely continuous map $\xi\colon I \to \mathbb{R}^n$ is a *solution of (27) on I generated by u* if $I \subseteq J$ is an interval and $\dot{\xi}(t) \in f(\xi(t),u(t)) + [\![-w,w]\!]$ holds for almost every $t \in I$. Whenever u is constant on I with value $\bar{u} \in U$, we slightly abuse the language and refer to ξ as a solution of (27) on I generated by $\bar{u}$.

We consider the following optimal control problem associated with the sampled behavior of (27).

VII.1 Definition. Given a sampling time $\tau > 0$ and cost functions

$$g_1\colon \mathbb{R}^n \times \mathbb{R}^n \times U \to \mathbb{R}_+ \cup \{\infty\}, \quad G_1\colon \mathbb{R}^n \to \mathbb{R}_+ \cup \{\infty\},$$

the tuple $\Pi_1 = (X_1,U_1,F_1,G_1,g_1)$ is the *optimal control problem associated with (27) and τ*, where $X_1 = \mathbb{R}^n$, $U_1 = U$, and $F_1\colon X_1 \times U_1 \rightrightarrows X_1$ is implicitly defined by $x' \in F_1(x,u)$ iff there exists a solution ξ of (27) on $[0,\tau]$ generated by $u \in U$ that satisfies $\xi(0) = x$ and $\xi(\tau) = x'$. □

The following hypothesis ensures that Π_1 is actually an optimal control problem in the sense of Definition III.3 that additionally satisfies Hypothesis (A_2), i.e., a problem to which our results in Section VI apply.

($\mathbf{A_4}$) The input set satisfies $U = \cup_{i\in[1;l]} [\![\check{u}_i,\hat{u}_i]\!]$, with $\check{u}_i,\hat{u}_i \in \mathbb{R}^m$, $\check{u}_i \leq \hat{u}_i$, and $l \in \mathbb{N}$. The function G_1 and g_1 is continuous on the set $G_1^{-1}(\mathbb{R})$ and $g_1^{-1}(\mathbb{R})$, respectively, and these sets are open. The map f is continuous, and for all $i,j \in [1;n]$, the partial derivative $D_j f_i$ with respect to the jth component of the first argument of f_i exists and is continuous. Every solution ξ of (27) on $[0,s]$ generated by some $u \in U$, where $s < \tau$, can be extended to a solution on $[0,\tau]$ generated by u.

VII.2 Lemma (Lemma 1 [31]). Consider an optimal control problem $\Pi_1 = (X_1,U_1,F_1,G_1,g_1)$ associated with (27) and $\tau > 0$ and suppose that (A_4) holds. Then Π_1 is an optimal control problem that satisfies (A_2). □

For the actual computation of abstractions, we introduce the *domain* K of (X_1,U_1,F_1,G_1,g_1),

$$\begin{aligned} K = \{p \in X_1 \mid g_1(X_1,p,U_1) \cup \\ g_1(p,X_1,U_1) \cup \{G_1(p)\} \neq \{\infty\}\} \end{aligned} \tag{28}$$

which includes the effective domain of the value function.

In the construction of an abstraction of the optimal control problem associated with (27) various bounds related to the dynamics and the cost functions are used, as detailed below. Here and in Section VIII, $|x|$ and $\|x\|$ denote the component-wise absolute value, respectively, the infinity norm of $x \in \mathbb{R}^n$, and all balls are understood with respect to the infinity norm.

($\mathbf{A_5}$) Let K be defined by (28). Let K' be convex and compact and so that for every $u \in U$ and every solution ξ of (27) on $[0,\tau]$ generated by u with $\xi(0) \in K$ we have $\xi([0,\tau]) \subseteq K'$. The constants $A_0 \in \mathbb{R}^n_+$, $A_1 \in \mathbb{R}^{n\times n}$, $A_2,A_3 \geq 0$ and $\varepsilon > 0$ satisfy the inequalities (component-wise)

$$A_0 \geq |f(p,u)| + w, \tag{29a}$$

$$(A_1)_{i,j} \geq \begin{cases} D_j f_i(x,u), & \text{if } i = j, \\ |D_j f_i(x,u)|, & \text{otherwise} \end{cases} \tag{29b}$$

for all $u \in U$ and all $p \in \bar{B}(K',\varepsilon)$. Moreover, for all $p,\bar{p} \in G_1^{-1}(\mathbb{R})$ we have

$$\|p-\bar{p}\|A_2 \geq |G_1(p) - G_1(\bar{p})|, \tag{29c}$$

and for all $(p,q,u),(\bar{p},\bar{q},u) \in g_1^{-1}(\mathbb{R})$ we have

$$(\|p-\bar{p}\| + \|q-\bar{q}\|)A_3 \geq |g_1(p,q,u) - g_1(\bar{p},\bar{q},u)|. \tag{29d}$$

We refer the interested reader to [31] for a discussion of the computation of the quantities in (A_5).

Following [31], an abstraction Π_2 of the optimal control problem Π_1 associated with (27) and τ is obtained as follows. Let Π_1 and Π_2 be of the form (16). The state alphabet X_2 is constructed from a uniform discretization of the domain (28) of Π_1 using the discretization parameter $\eta \in (\mathbb{R}_+ \setminus \{0\})^n$. Similarly, the input alphabet U_2 is obtained by a discretization of U_1 using the discretization parameter $\mu \in (\mathbb{R}_+ \setminus \{0\})^n$. The

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2018.2863178, IEEE Transactions on Automatic Control

Table I
PARAMETERS OF THE COMPUTATION OF THE ABSTRACTION IN [31].

$\eta \in (\mathbb{R}_+ \smallsetminus \{0\})^n$	state alphabet discretization
$\mu \in (\mathbb{R}_+ \smallsetminus \{0\})^m$	input alphabet discretization
$k \in \mathbb{N}$	sample interval discretization
$\theta > 0$	subdivision factor
$\gamma > 0$	bound on numerical errors

transition function F_2 is obtained from an over-approximation of the attainable set of (27) whose computation is outlined in Algorithm 1 in [31]. To this end, the sampling time τ is subdivided in k inter-sampling times $t = \tau/k$. At each of those inter-sampling times, the attainable set is over-approximated by a union of hyper-intervals using a *growth bound* [2, Def. VIII.2], [50] to bound the distance of neighboring trajectories. Here the estimates A_0 and A_1 in (A_5) are instrumental. In order to control the error due to the over-approximation, at each inter-sampling time, each hyper-interval in the approximation can be subdivided in smaller hyper-intervals, whose size is determined by the parameter $\theta > 0$. Throughout the computation, several initial value problems have to be solved numerically. The resulting error together with other errors, e.g. rounding errors, can be accounted for using the parameter $\gamma > 0$. The cost functions G_2, g_2 of the abstraction are derived from the values of the cost functions G_1, g_1 evaluated at the discretized states and inputs. The Lipschitz constants in (29c) and (29d) are used to ensure that the functions G_2, g_2 indeed are upper bounds in the sense of (ii) and (iii) in Proposition VI.2. The parameters of the construction of the abstraction in [31] are summarized in Tab. I.

We use Π to refer to the optimal control problem associated with (27) and τ, and we consider sequences of parameters in Tab. I satisfying

$$\lim_{i\to\infty} \eta_i = 0, \lim_{i\to\infty} \mu_i = 0, \lim_{i\to\infty} \left(\theta_i \|\eta_i\| + \frac{1}{k_i} + \gamma_i k_i \right) = 0.$$

Then the method in [31, Sec. V] produces a sequence $(\Pi_i)_{i\in\mathbb{N}}$ of finite abstractions Π_i of some conservatism $\rho_i \in \mathbb{R}_+ \cup \{\infty\}$ of Π, satisfying $\lim_{i\to\infty} \rho_i = 0$, as required in hypothesis (A_3) in Section VI-C. See [31, Th. 1, 2].

B. Solution of finite optimal control problems

We propose Algorithm 1 to efficiently solve the optimal control problem (7) whenever the state and input alphabets are finite; see Theorem VII.3 below. The algorithm can be regarded as an implementation of the high-level algorithm in [40], with improved run time bound and suitable modifications to additionally compute a controller realizing the achievable closed-loop performance. We also present a condition under which the run time is linear in the size of the abstraction of the plant. This result applies e.g. to the Reach-Avoid and Minimum Time Problems in Examples III.5 and III.6, and contains the unweighted case of [51] as a special case. In the following, $\mathrm{card}(M)$ denotes the cardinality of the set M.

VII.3 Theorem. Let (7) be an optimal control problem with finite X and U. Then Algorithm 1 terminates.
Suppose that the maps c and W are returned on termination,

Algorithm 1 Dijkstra-like algorithm to solve finite problems

Input: Optimal control problem (X, U, F, G, g)
Require: X, U finite
1: $W := G$ // value function
2: $Q := \{x \in X \mid G(x) < \infty\}$ // priority queue
3: $E := \varnothing$ // set of settled states
4: **for all** $p \in X$ **do**
5: $\quad c(p) := \varnothing$ // controller
6: **while** $Q \neq \varnothing$ **do**
7: $\quad q :\in \mathrm{argmin}\,\{W(x) \mid x \in Q\}$
8: $\quad Q := Q \setminus \{q\}$
9: $\quad E := E \cup \{q\}$
10: $\quad$ **for all** $(p, u) \in F^{-1}(q)$ **do**
11: $\quad\quad M := \max\{g(p, y, u) + W(y) \mid y \in F(p, u)\}$
12: $\quad\quad$ **if** $F(p, u) \subseteq E$ and $W(p) > M$ **then**
13: $\quad\quad\quad W(p) := M$
14: $\quad\quad\quad Q := Q \cup \{p\}$
15: $\quad\quad\quad c(p) := \{u\}$
Output: c, W

and let $C = (Z, Z, X, U, H)$, where Z is any singleton set, $u_0 \in U$, and $H : Z \times X \rightrightarrows Z \times U \times \{0, 1\}$ is given by

$$H(Z, p) = \begin{cases} Z \times \{u_0\} \times \{1\}, & \text{if } c(p) = \varnothing, \\ Z \times c(p) \times \{0\}, & \text{otherwise.} \end{cases} \tag{30}$$

Then C is a static controller for S, and $L = V = W$, where S, L and V denote the system (4), the closed-loop value function of (7) associated with C, and the value function of (7). Moreover, Algorithm 1 can be implemented such that it runs in $O(m + n \log n)$ time, where $n = \mathrm{card}(X)$ and $m = \sum_{p\in X} \sum_{u\in U} \mathrm{card}(F(p, u))$, and in $O(m)$ time if additionally

$$g(X, X, U) \subseteq \{\gamma, \infty\} \text{ and } G(X) \subseteq \{\Gamma, \gamma + \Gamma, \infty\} \tag{31}$$

for some $\gamma, \Gamma \in \mathbb{R}_+$. □

Proof. Observe that $M \geq W(q)$, and in turn, $p \neq q$, on lines 13-15. Thus, throughout the algorithm on lines 8-15, the value of $W(q)$ monotonically increases and $W(q) \geq \max W(E)$. Then $p \notin E$ on lines 13-15, and so each q is removed from Q at most once. This shows that the `while`-loop on lines 6-15 is entered at most n times. Moreover, $F^{-1}(q) \subseteq X \times U$ on line 10, and so the algorithm terminates as $X \times U$ is finite.

Next note that W is a monotonically decreasing sequence of functions $X \to [0, \infty]$ bounded above by G. Using induction we see that $Q \cup E = W^{-1}(\mathbb{R}_+)$ on line 15.

If $W \geq V$, then $M \geq P(V)(p)$ on line 13, where P is the dynamic programming operator associated with (7), and so $W \geq V$ on lines 6-15 throughout the algorithm, as $V = P(V)$ by Th. IV.1. We claim that $W \leq P(W)$ upon termination, which implies $W = V$ by Th. IV.1. Assume the contrary. Then, as $W \leq G$, there exist $(p, u) \in X \times U$ such that

$$W(p) > \max\{g(p, y, u) + W(y) \mid y \in F(p, u)\}, \tag{32}$$

and in turn, $F(p, u) \subseteq E$ since $E = W^{-1}(\mathbb{R}_+)$. Let $q \in F(p, u)$ be the element that is last added to E. Then, upon its addition on line 9 we have $W(p) > M \geq W(q)$ on line 12

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2018.2863178, IEEE Transactions on Automatic Control

by (32). Thus, line 13 is executed, which contradicts (32) and so implies that $W = V$ upon termination.

Obviously, C is a static controller for S. To show that $L = W$ upon termination, first suppose that $q \notin E$ upon termination. Then $W(q) = \infty$ and $c(q) = \varnothing$, and so $L(q) = \infty$ by (30). Hence, it suffices to show that $L(q) = W(q)$ on line 9 throughout the algorithm. To this end, we proceed by induction and assume that $L(x) = W(x)$ holds on line 8 for all $x \in E$. Note that $c(q) \neq \varnothing$ since line 14 must have been executed at least once, and additionally

$$W(q) = \max \{ g(q, y, c(q)) + L(y) \mid y \in F(q, c(q)) \} . \quad (33)$$

Then $v(0) = 0$ for every $(u, v, x) \in \mathcal{B}_q(C \times S)$ by (30), and in turn, $J(u, v, x) = g(q, x(1), c(q)) + J(\sigma u, \sigma v, \sigma x)$. Then $L(q) = W(q)$ by (33).

The data G, W, E and c are maintained as arrays, so the respective operations in the algorithm require unit time. Given an adjacency lists representation [39] of F that also stores the map g, both an analogous representation of F^{-1} can be obtained and the condition (31) can be verified, in $O(m)$ time.

Lines 11-15 are executed at most m times. Using auxiliary counters the tests $F(p, u) \subseteq E$ on line 12 take $O(m)$ total time [51], and analogously for computing the maximum on line 11. Thus, Algorithm 1 requires $O(m)$ time, plus the time for executing line 2, executing lines 7, 8 and 14 at most n times, and for executing line 13 at most m times. Consequently, the first time bound is met if Q is maintained as a Fibonacci heap [39]. If condition (31) holds, then $M = \gamma + W(q)$ on line 13, and so $W(Q) \subseteq \{W(q), \gamma + W(q)\}$ on line 8. Thus, the second bound is met if Q is maintained as a FIFO queue [39]. □

C. Comments on Computational Complexity

In our approach, the concrete control problem (7) is discretized first, resulting in an abstration which is solved subsequently. Bounds on the computational complexity have been provided in Theorem VII.3 for the second step, and in [52, Sec. III.D], for the special case of the first step when $k = 1$ and η, μ, Θ and γ are constants. The estimates show that the overall computational effort is enormous and has to be expected to grow rapidly with the dimension of X, and even more acutely so when a sequence of abstractions of decreasing conservatism is to be computed. While the problem is found with all discretization based methods to solve (7), several strategies to somewhat relieve the computational burden that have been proposed, e.g. [53]–[55], could potentially be extended to our setting.

VIII. Illustrative Examples and Applications

We shall demonstrate our approach on three optimal control problems. In every of these three cases, and in contrast to the theory presented in this paper, none of the related works discussed in Section I is capable of synthesizing controllers together with upper bounds on their performances that arbitrarily closely approximate the best achievable performance.

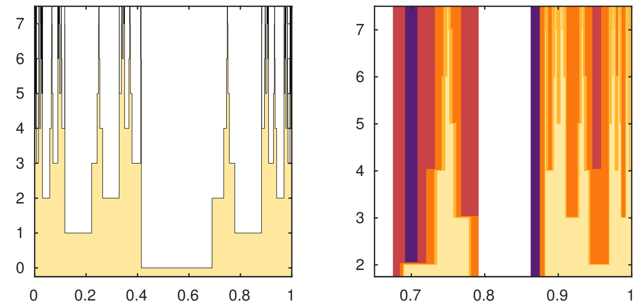

Figure 4. Minimum time problem involving chaotic dynamics. Left: Hypograph of the value function V. Right: Hypographs of V (light yellow) and of the approximate value functions V_N for $N \in \{40, 60, 85, 400\}$ (purple, red, orange and dark yellow, respectively).

A. A minimum time problem involving chaotic dynamics

To demonstrate the capability of our theory to approximate complex value functions, we first apply it to an instance Π of the Minimum Time Problem in Example III.6 whose underlying dynamics is chaotic. Specifically, $\Pi = ([0,1], \{0\}, F, G, g)$, where the transition function F is the *logistic map* [56], $F(p, 0) = \{4p(1-p)\}$, and the target and obstacle sets are given by $D =]0.415, 0.69[$ and $M = \varnothing$.

The value function V of Π is discontinuous and rather irregular, see Fig. 4, but can be determined exactly by rewriting the iteration in Corollary IV.2 into an iteration for sublevel sets, $V^{-1}(0) = D$ and $V^{-1}([0; T+1]) = F(\cdot, 0)^{-1}(V^{-1}([0; T]))$.

For everyy $N \in \mathbb{N}$ it is straightforward to compute an abstraction $\Pi_N = (X_N, \{0\}, F_N, G_N, g_N)$ of conservatism $1/N$ of Π, where F_N satisfies the conditions in Def. VI.3,

$$\begin{aligned} X_N &= \{\Omega_0, \dots, \Omega_N\}, \\ \Omega_i &= \left(\tfrac{i}{N} + \left[-\tfrac{1}{2N}, \tfrac{1}{2N} \right] \right) \cap [0,1] , \\ g_N(\Omega, \Omega', 0) &= 1, \text{ and} \\ G_N(\Omega) &= \begin{cases} 0, & \text{if } \Omega \subseteq D, \\ \infty, & \text{otherwise,} \end{cases} \end{aligned}$$

for all $i \in [0; N]$ and all $\Omega, \Omega' \in X_N$. The value function V_N of Π_N is easily computed using Algorithm 1 in Section VII-B. Fig. 4 illustrates the approximation of V by V_N, for selected values of the conservatism $1/N$.

B. An entry-time problem for the inverted pendulum

We consider a variant of the popular inverted pendulum problem with perturbations, where the motion of the cart is not modeled; see e.g. [52], [57]. The acceleration u of the cart, which is constrained to $[-2, 2]$, is the input to the system

$$\dot{x}_1 = x_2 \quad (34a)$$
$$\dot{x}_2 \in \sin(x_1) + u \cos(x_1) - 2\kappa x_2 + [-w, w] , \quad (34b)$$

the states x_1 and x_2 correspond to the angle, respectively, the angular velocity of the pole, $\kappa = 0.01$ is a friction coefficient, and $w = 0.1$ accounts for any uncertainties.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2018.2863178, IEEE Transactions on Automatic Control

We restrict the domain of the problem to $K =]-2\pi, 2\pi[\times]-3, 3[$, i.e., the set $\mathbb{R}^2 \setminus K$ is an obstacle, and choose a neighborhood D of the upwards pointing equilibrium $(0, 0)$,

$$D = \left\{ x \in \mathbb{R}^2 \,\middle|\, 63x_1^2 + 12x_2x_1 + 56x_2^2 < 42 \right\},$$

as the target set. In correspondence with K and D, we define the terminal and running cost functions G and g by $G(p) = 0$ if $p \in D \cap K = D$, $G(p) = \infty$, otherwise, and

$$g(p, q, u) = \begin{cases} u^2, & \text{if } p \in K, \\ \infty, & \text{otherwise.} \end{cases}$$

We use Π to refer to the optimal control problem associated with the system (34), the sampling time $\tau = 0.2$ and the cost functions G and g. With Π we aim at minimizing the actuation energy to steer the system into the target D. We pick the constants in (A_5) to

$$A_0 := \begin{pmatrix} 4 \\ 2.5 \end{pmatrix}, \; A_1 := \begin{pmatrix} 0 & 1 \\ 2.25 & -0.02 \end{pmatrix}, \; A_2 := 0, \; A_3 := 0.$$

We use A_0 to verify that $K' = \bar{B}(\mathrm{cl}K, 0.9)$ contains any solution of (34) originating form K since $\bar{B}(K, \tau\|A_0\|) \subseteq K'$. Moreover, (29) is satisfied on $[-8, 8] \times [-4, 4] \supseteq \bar{B}(K', 0.1)$, and we see that ($A_5$) holds for $\varepsilon = 0.1$.

We conducted several experiments using $\theta = 1$ and four parameter tuples (η, μ, k) with values $p_1 = ((0.08, 0.08), 0.2, 1)$, $p_2 = ((0.04, 0.04), 0.15, 2)$, $p_3 = ((0.02, 0.02), 0.1, 3)$ and $p_4 = ((0.01, 0.01), 0.05, 4)$. For the solution of initial value problems, which are necessary in the construction of the abstraction [31], we use the Taylor series method [58] of order 5 with stepsize $\tau/(5k)$. We use γ to account for any numerical errors, which we derive from the 6th order remainder term of the Taylor expansion maximized over the appropriate domain. Specifically, for $k = 1$, $k = 2$, $k = 3$ and $k = 4$ we obtain $\gamma = 6.3 \cdot 10^{-7}$, $\gamma = 9.9 \cdot 10^{-9}$, $\gamma = 8.7 \cdot 10^{-10}$ and $\gamma = 1.6 \cdot 10^{-10}$, respectively. The computation time to compute the abstraction Π_i and the optimal controller C_i (Alg. 1) is 0.5, 8.5, 139 and 4715 seconds, for the parameter tuple p_i, $i \in [1; 4]$, respectively. (Here and for the following example, computations are conducted on 3.5 GHz Intel Core i7 CPU with 32GB memory.) The performance of the controllers $C_1 \circ \in$ through $C_4 \circ \in$ is illustrated in Fig. 5.

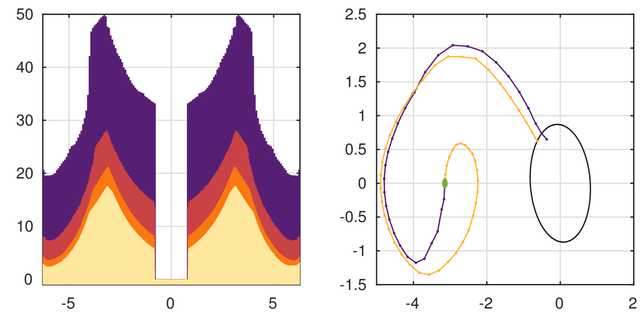

Figure 5. Entry-time problem for the inverted pendulum. Left: Cross-section of the hypograph of the closed-loop value function of Π associated with the controller $C_i \circ \in$, ranging over $x_1 \in [-2\pi, 2\pi]$ for fixed $x_2 = 0$, for $i \in \{1, 2, 3, 4\}$ (purple, red, orange and yellow, respectively). Right: Closed-loop trajectories generated by the controllers $C_1 \circ \in$ (purple) and $C_4 \circ \in$ (yellow); the closed-loop value function at the initial states is bounded by 47.68, respectively, 17.65. The initial position is marked by the green dot and the target set D is illustrated by the black ellipse.

C. The Homicidal Chauffeur Game

In this pursuit-evasion game, a car with restricted turning radius, traveling at some constant velocity, aims at catching an agile pedestrian as quickly as possible [42]. The problem can be posed as a Minimum Time Problem by choosing the center of the car as origin and directing the y axis along the velocity vector of the car. The dynamics is then described by

$$\begin{aligned} \dot{x} &= -yu + v_1 \\ \dot{y} &= xu - 1 + v_2, \end{aligned}$$

where the input $|u| \leq 1$ is the forward velocity of the car, and $v = (v_1, v_2)$ is the velocity vector of the pedestrian [42], which we consider as a perturbation with bound $\|v\| \leq 0.3$. Using the sampling time $\tau = 0.1$ and the domain $K =]-5, 5[\times]-5, 5[$, we cast the sampled differential game as Minimum Time Problem with target set $D = \left\{ (x, y) \in \mathbb{R}^2 \,\middle|\, x^2 + y^2 < 0.9 \right\}$ and the obstacle set $M = \mathbb{R}^2 \setminus K$. The cost functions follow according to Example III.6 and it is straightforward to verify the Hypothesis (A_5) as follows. We fix $\varepsilon = 0.1$, $A_0 = (6.4, 6.4)$, and $(A_1)_{11} = (A_1)_{22} = 0$, $(A_1)_{12} = (A_1)_{21} = 1$, $A_2 = A_3 = 0$ and $K' = [-6, 6] \times [-6, 6]$. The estimates (29) are obvious, and (29a) implies that every solution ξ on $[0, \tau]$ evolves inside $\bar{B}(K, \tau\|A_0\|) \subseteq K'$, and so ($A_5$) holds.

We approximately solve Π using $\theta = 2$ and four parameter tuples (η, μ, k) with values $p_1 = ((0.03, 0.03), 0.2, 1)$, $p_2 = ((0.02, 0.02), 0.1, 2)$, $p_3 = ((0.015, 0.015), 0.1, 3)$ and $p_4 = ((0.01, 0.01), 0.05, 4)$. As the nominal dynamics under constant control inputs can be solved exactly, we neglect the numerical errors and set $\gamma = 0$. The computation time to compute the abstraction Π_i and the optimal controller C_i (Alg. 1) is 3.5, 34, 133 and 1851 seconds, for the parameter tuple p_i, $i \in [1; 4]$, respectively. Naturally, with finer discretization parameters the computation times increases. The performance of the controllers $C_1 \circ \in$ through $C_4 \circ \in$ is illustrated in Fig. 6.

IX. Summary and Conclusions

We have presented a novel approach to solve a class of leavable, undiscounted optimal control problems in the minimax sense for nonlinear control systems in the presence of perturbations and constraints. The approach is correct-by-construction, i.e., the closed-loop value function of the synthesized controller is upper bounded by the closed-loop value function of the abstract controller. Compared to previously known results, our approach is applicable to more general cost functions and plant dynamics, and the resulting controllers are memoryless and symbolic. Moreover, as we have shown, the closed-loop value function associated with the concrete controller hypo-converges to the concrete value function as the conservatism of the abstraction approaches zero. This powerful convergence result distinguishes itself form previously known results in several important aspects. Most notably, it applies to discontinuous value functions and implies that our approach is complete in a well-defined sense.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2018.2863178, IEEE Transactions on Automatic Control

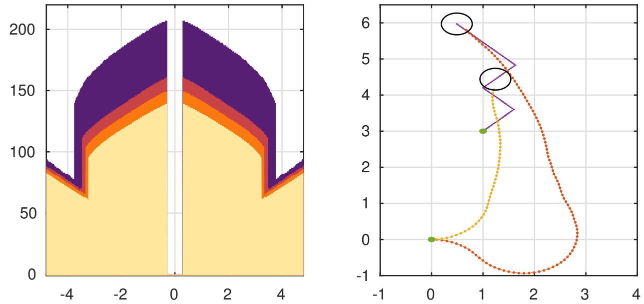

Figure 6. Homicidal Chauffeur Game. Left: Cross-section of the hypograph of the closed-loop value function of Π associated with $C_i \circ \in$, ranging over $x \in [-4.5, 4.5]$ for fixed $y = 0$, for $i \in \{1, 2, 3, 4\}$ (purple, red, orange and yellow, respectively). Right: Simulation of the closed-loop. The position of the pedestrian (evader) is illustrated in purple. The position of the car (pursuer) for $C_1 \circ \in$ and $C_4 \circ \in$ is shown in red, respectively, yellow. The initial positions are marked by the green squares, and the capture radius 0.3 is indicated by the black circles. The worst-case capture times from the initial state for $C_1 \circ \in$ and $C_4 \circ \in$ are bounded by 17.0, respectively, 5.3 seconds.

We have illustrated our results on three optimal control problems, two of which involving discrete-time plants that represent the sampled behavior of continuous-time, nonlinear control systems with additive disturbances. Here, we employed an algorithm that we have proposed in [31], to compute abstractions of arbitrary conservatism. To increase the computational efficiency of the overall synthesis approach proposed in this paper is a subject of our current research.

Appendix

A. The Notion of Hypo-Convergence

The result below shows that, for the special case considered in Definition VI.7, that definition is equivalent to respective definitions in the literature [33, Ch. 7.B], [34, Cor. VII.5.26].

A.1 Proposition. Let X, V and L be as in Definition VI.7. Then $V = \text{h-lim}_{i\to\infty} L_i$ iff $\limsup_{i\to\infty} L_i(x_i) \leq V(p)$ for every $p \in X$ and every sequence $(x_i)_{i\in\mathbb{N}}$ converging to p. $\square$

Proof. For sufficiency, let $p \in X$ and $\varepsilon > 0$, and assume that the condition in Definition VI.7 does not hold. Then there exists a sequence $(x_i)_{i\in\mathbb{N}}$ in X converging to p and satisfying $L_i(x_i) > V(p) + \varepsilon/2$ for infinitely many $i \in \mathbb{N}$. This implies $\limsup_{i\to\infty} L_i(x_i) > V(p)$, which is a contradiction. For necessity, assume that the latter inequality holds for some $p \in X$ and some sequence $(x_i)_{i\in\mathbb{N}}$ in X converging to p. Then $L_i(x_i) \geq \lambda > V(p)$ for some $\lambda \in \mathbb{R}$ and infinitely many $i \in \mathbb{N}$. In addition, as V is u.s.c., there exists $\varepsilon > 0$ such that $V(q) < \lambda - \varepsilon$ for all $q \in B(p, 2\varepsilon)$. As $V = \text{h-lim}_{i\to\infty} L_i$ there exists a neighborhood $N \subseteq X$ of p such that (24) holds for all sufficiently large $i \in \mathbb{N}$. Then there exists some i such that $x_i \in B(p, \varepsilon)$ and $(x_i, \lambda) \in B(\operatorname{hypo} V, \varepsilon)$. In turn, there exists $(q, \alpha) \in \operatorname{hypo} V$ such that $\lambda < \alpha + \varepsilon$ and $x_i \in B(q, \varepsilon)$. This implies $q \in B(p, 2\varepsilon)$, hence $\alpha \leq V(q) < \lambda - \varepsilon$, which is a contradiction. $\square$

B. Some Results on Semi-Continuous Maps

Throughout, X and Y are metric spaces. See [34], [59].

A.2 Theorem (Berge's Maximum Theorem). Let $H : X \rightrightarrows Y$ be compact-valued and u.s.c., and let $f : X \times Y \to [-\infty, \infty]$ be u.s.c.. Then the map $g : X \to [-\infty, \infty]$ defined by $g(x) = \sup\{f(x, y) \mid y \in H(x)\}$ is u.s.c.. $\square$

A.3 Proposition. Let $\Omega \subseteq X$ be compact, and suppose that the sequence $(f_k)_{k\in\mathbb{N}}$ of u.s.c. maps $f_k : X \to [-\infty, \infty]$ is monotonically decreasing and converges pointwise to $g : X \to [-\infty, \infty]$. Then $\lim_{k\to\infty} \sup_{x\in\Omega} f_k(x) = \sup_{x\in\Omega} g(x)$, where limits are understood to take values in $[-\infty, \infty]$. $\square$

A.4 Proposition. The map $H : X \rightrightarrows Y$ is compact-valued and u.s.c. iff the following condition holds:
If $(x_k, y_k)_{k\in\mathbb{N}}$ is a sequence in the graph of H and $(x_k)_{k\in\mathbb{N}}$ converges to $p \in X$, then there exists a subsequence of $(y_k)_{k\in\mathbb{N}}$ converging to some point in $H(p)$. $\square$

A.5 Corollary. If the map $H : X \rightrightarrows Y$ is compact-valued and u.s.c., then $H(\Omega)$ is compact for all compact subsets $\Omega \subseteq X$.

References

[1] P. Tabuada, *Verification and control of hybrid systems*. Springer, 2009.

[2] G. Reissig, A. Weber, and M. Rungger, "Feedback refinement relations for the synthesis of symbolic controllers," *IEEE Trans. Automat. Control*, vol. 62, no. 4, pp. 1781–1796, Apr. 2017, http://dx.doi.org/10.1109/TAC.2016.2593947.

[3] C. Belta, B. Yordanov, and E. A. Gol, *Formal methods for discrete-time dynamical systems*, ser. Studies in Systems, Decision and Control. Springer, 2017, vol. 89.

[4] A. P. Maitra and W. D. Sudderth, *Discrete gambling and stochastic games*, ser. Applications of Mathematics (New York). Springer, 1996, vol. 32.

[5] M. Mazo, Jr. and P. Tabuada, "Symbolic approximate time-optimal control," *Systems Control Lett.*, vol. 60, no. 4, pp. 256–263, 2011.

[6] A. Girard, "Controller synthesis for safety and reachability via approximate bisimulation," *Automatica J. IFAC*, vol. 48, no. 5, pp. 947–953, 2012.

[7] F. de Roo and M. Mazo, "On symbolic optimal control via approximate simulation relations," in *Proc. IEEE Conf. Decision and Control (CDC), Florence, Italy, 10-13 Dec. 2013*, 2013, pp. 3205–3210.

[8] M. Broucke, M. D. Di Benedetto, S. Di Gennaro, and A. Sangiovanni-Vincentelli, "Efficient solution of optimal control problems using hybrid systems," *SIAM J. Control Optim.*, vol. 43, no. 6, pp. 1923–1952, 2005.

[9] Y. Tazaki and J.-i. Imura, "Discrete abstractions of nonlinear systems based on error propagation analysis," *IEEE Trans. Automat. Control*, vol. 57, no. 3, pp. 550–564, 2012.

[10] Y. P. Leong and P. Prabhakar, "Optimal control with regular objectives using an abstraction-refinement approach," in *Proc. American Control Conference (ACC), Boston, MA, U.S.A., 6-8 Jul. 2016*, 2016, pp. 5161–5168.

[11] R. E. Bellman and S. E. Dreyfus, *Applied dynamic programming*. Princeton University Press, Princeton, N.J., 1962.

[12] D. P. Bertsekas and S. E. Shreve, *Stochastic optimal control: The discrete time case*. Athena Scientific, Belmont, MA, 1996.

[13] D. P. Bertsekas, *Abstract dynamic programming*. Athena Scientific, Belmont, MA, 2013.

[14] Y. Jiang and Z.-P. Jiang, "Robust adaptive dynamic programming and feedback stabilization of nonlinear systems," *IEEE Trans. Neural Networks and Learning Systems*, vol. 25, no. 5, pp. 882–893, May 2014.

[15] A. Heydari, "Theoretical and numerical analysis of approximate dynamic programming with approximation errors," *J. Guidance Control Dynam.*, vol. 39, no. 2, pp. 301–311, Feb. 2016.

[16] O. Bokanowski, N. Forcadel, and H. Zidani, "Reachability and minimal times for state constrained nonlinear problems without any controllability assumption," *SIAM J. Control Optim.*, vol. 48, no. 7, pp. 4292–4316, 2010.

[17] J. F. Fisac, M. Chen, C. J. Tomlin, and S. S. Sastry, "Reach-avoid problems with time-varying dynamics, targets and constraints," in *Proc. 18th Intl. Conf. Hybrid Systems: Computation and Control (HSCC), Seattle, WA, U.S.A., Apr.14-16, 2015*. ACM, 2015, pp. 11–20.

[18] K. Margellos and J. Lygeros, "Viable set computation for hybrid systems," *Nonlinear Anal. Hybrid Syst.*, vol. 10, pp. 45–62, 2013.

[19] H. J. Kushner and P. G. Dupuis, *Numerical methods for stochastic control problems in continuous time*, ser. Applications of Mathematics (New York). Springer, 1992, vol. 24.

[20] D. P. Bertsekas and J. N. Tsitsiklis, *Neuro-Dynamic Programming*. Athena Scientific, Belmont, MA, 1996.

[21] F. Dufour and T. Prieto-Rumeau, "Approximation of Markov decision processes with general state space," *J. Math. Anal. Appl.*, vol. 388, no. 2, pp. 1254–1267, 2012.

[22] N. Saldi, S. Yüksel, and T. Linder, "On the asymptotic optimality of finite approximations to Markov decision processes with Borel spaces," *Math. Oper. Res.*, vol. 42, no. 4, pp. 945–978, 2017.

[23] G. Kreisselmeier and T. Birkhölzer, "Numerical nonlinear regulator design," *IEEE Trans. Automat. Control*, vol. 39, no. 1, pp. 33–46, 1994.

[24] M. Korda, D. Henrion, and C. N. Jones, "Controller design and value function approximation for nonlinear dynamical systems," *Automatica J. IFAC*, vol. 67, pp. 54–66, 2016.

[25] M. Bardi, S. Bottacin, and M. Falcone, "Convergence of discrete schemes for discontinuous value functions of pursuit-evasion games," in *New trends in dynamic games and applications*, ser. Ann. Internat. Soc. Dynam. Games, 1995, vol. 3, pp. 273–304.

[26] P. Cardaliaguet, M. Quincampoix, and P. Saint-Pierre, "Set-valued numerical analysis for optimal control and differential games," in *Stochastic and differential games*, ser. Ann. Internat. Soc. Dynam. Games. Boston, MA: Birkhäuser Boston, 1999, vol. 4, pp. 177–247.

[27] L. Grüne and O. Junge, "Approximately optimal nonlinear stabilization with preservation of the Lyapunov function property," in *Proc. 46th IEEE Conf. Decision and Control (CDC), New Orleans, LA, U.S.A., 2007*, 2007, pp. 702–707.

[28] L. Grüne and O. Junge, "Global optimal control of perturbed systems," *J. Optim. Theory Appl.*, vol. 136, no. 3, pp. 411–429, 2008.

[29] S. Karaman and E. Frazzoli, "Sampling-based algorithms for optimal motion planning," *Internat. J. Robotics Res.*, vol. 30, no. 7, pp. 846–894, Jun. 2011.

[30] Y. Li, Z. Littlefield, and K. E. Bekris, "Asymptotically optimal sampling-based kinodynamic planning," *Internat. J. Robotics Res.*, vol. 35, no. 5, pp. 528–564, 2016.

[31] M. Rungger and G. Reissig, "Arbitrarily precise abstractions for optimal controller synthesis," in *Proc. 56th IEEE Conf. Decision and Control (CDC), Melbourne, Australia, 12-15 Dec. 2017*, 2017, pp. 1761–1768, http://dx.doi.org/10.1109/CDC.2017.8263904.

[32] G. Reissig and M. Rungger, "Abstraction-based solution of optimal stopping problems under uncertainty," in *Proc. IEEE Conf. Decision and Control (CDC), Florence, Italy, 10-13 Dec. 2013*, 2013, pp. 3190–3196, http://dx.doi.org/10.1109/CDC.2013.6760370.

[33] R. T. Rockafellar and R. J.-B. Wets, *Variational analysis*, ser. Grundlehren der Mathematischen Wissenschaften. Berlin: Springer-Verlag, 1998, vol. 317, 3rd corr printing 2009.

[34] S. Hu and N. S. Papageorgiou, *Handbook of multivalued analysis. Vol. I*, ser. Mathematics and its Applications. Kluwer, 1997, vol. 419.

[35] H. Choset, K. Lynch, S. Hutchinson, G. Kantor, W. Burgard, L. Kavraki, and S. Thrun, *Principles of Robot Motion: Theory, Algorithms, and Implementations*. Cambridge, MA, USA: MIT Press, 2005.

[36] M. Bardi and I. Capuzzo-Dolcetta, *Optimal control and viscosity solutions of Hamilton-Jacobi-Bellman equations*, ser. Systems & Control: Foundations & Applications. Birkhäuser, 1997.

[37] S. Coogan, M. Arcak, and C. Belta, "Formal methods for control of traffic flow," *IEEE Control Syst. Mag.*, vol. 37, no. 2, pp. 109–128, 2017.

[38] S. M. LaValle, *Planning algorithms*. Cambridge University Press, 2006.

[39] R. K. Ahuja, T. L. Magnanti, and J. B. Orlin, *Network flows*. Prentice Hall Inc., 1993.

[40] D. E. Knuth, "A generalization of Dijkstra's algorithm," *Information Processing Lett.*, vol. 6, no. 1, pp. 1–5, 1977.

[41] G. Gallo, G. Longo, S. Pallottino, and S. Nguyen, "Directed hypergraphs and applications," *Discrete Appl. Math.*, vol. 42, no. 2-3, pp. 177–201, 1993.

[42] R. Isaacs, *Differential games. A mathematical theory with applications to warfare and pursuit, control and optimization*. Wiley, 1965.

[43] A. E. Bryson, Jr. and Y. C. Ho, *Applied optimal control*. Wiley, 1975, optimization, estimation, and control, Revised printing.

[44] D. P. Bertsekas, "Value and policy iterations in optimal control and adaptive dynamic programming," *IEEE Trans. Neural Networks and Learning Systems*, vol. 28, no. 3, pp. 500–509, 2017.

[45] L. E. Dubins and L. J. Savage, *Inequalities for stochastic processes (how to gamble if you must)*. Dover, 1976.

[46] G. Reissig, "Approximate value iteration for a class of deterministic optimal control problems with infinite state and input alphabets," in *Proc. IEEE Conf. Decision and Control (CDC), Las Vegas, U.S.A., 12-14 Dec. 2016*, 2016, pp. 1063–1068, http://dx.doi.org/10.1109/CDC.2016.7798408.

[47] J. Liu, "Robust abstractions for control synthesis: Completeness via robustness for linear-time properties," in *Proc. 20th Intl. Conf. Hybrid Systems: Computation and Control (HSCC), Pittsburgh, Pennsylvania, USA, Apr. 18-20, 2017*, 2017, pp. 101–110.

[48] S. Kong, S. Gao, W. Chen, and E. Clarke, "dReach: δ-reachability analysis for hybrid systems," in *Proc. 21st Int. Conf. Tools Algorithms for the Construction and Analysis of Systems (TACAS), London, UK, 11-19 Apr., 2015*, C. Baier and C. Tinelli, Eds. Springer, 2015, pp. 200–205.

[49] M. Dellnitz and O. Junge, "Set oriented numerical methods for dynamical systems," in *Handbook of dynamical systems*, B. Fiedler, Ed. Amsterdam: North-Holland, 2002, vol. 2, pp. 221–264.

[50] T. Kapela and P. Zgliczyński, "A Lohner-type algorithm for control systems and ordinary differential inclusions," *Discrete Contin. Dyn. Syst. Ser. B*, vol. 11, no. 2, pp. 365–385, 2009.

[51] W. F. Dowling and J. H. Gallier, "Linear-time algorithms for testing the satisfiability of propositional Horn formulae," *J. Logic Programming*, vol. 1, no. 3, pp. 267–284, 1984.

[52] G. Reißig, "Computing abstractions of nonlinear systems," *IEEE Trans. Automat. Control*, vol. 56, no. 11, pp. 2583–2598, Nov. 2011, http://dx.doi.org/10.1109/TAC.2011.2118950.

[53] R. Munos and A. Moore, "Variable resolution discretization in optimal control," *Machine Learning*, vol. 49, no. 2, pp. 291–323, Nov. 2002.

[54] M. Rungger and O. Stursberg, "On-the-fly model abstraction for controller synthesis," in *American Control Conference (ACC)*, 2012, pp. 2645–2650.

[55] A. Weber, M. Rungger, and G. Reissig, "Optimized state space grids for abstractions," *IEEE Trans. Automat. Control*, vol. 62, no. 11, pp. 5816–5821, Nov. 2017, http://dx.doi.org/10.1109/TAC.2016.2642794.

[56] R. L. Devaney, *An introduction to chaotic dynamical systems*, 2nd ed., ser. Addison-Wesley Studies in Nonlinearity. Addison-Wesley, 1989.

[57] I. Fantoni and R. Lozano, *Non-linear control for underactuated mechanical systems*. Springer-Verlag, 2002.

[58] N. S. Nedialkov, K. R. Jackson, and G. F. Corliss, "Validated solutions of initial value problems for ordinary differential equations," *Appl. Math. Comput.*, vol. 105, no. 1, pp. 21–68, 1999.

[59] P. Kosmol and D. Müller-Wichards, *Optimization in function spaces*, ser. Series in Nonl. Anal. Appl. de Gruyter, 2011, vol. 13.

Gunther Reissig (S'93-M'99-SM'00) received his Dipl.-Ing. (EE), Dipl.-Math. and Dr.-Ing. (EE) degrees from the Technische Universität Dresden, Germany, in 1991, 1995, and 1998, respectively, and obtained the Facultas docendi and the Venia legendi in Systems Theory from the Technische Universität Berlin, Germany, in 2009. He has been with SIEMENS AG, Infineon Technologies and the Massachusetts Institute of Technology and is currently head of the Control Laboratory of the Chair of Control Engineering at the Bundeswehr University Munich, Germany. His research interests include theory and applications of continuous, discrete and hybrid dynamical systems, with a current focus on abstraction-based synthesis.

Matthias Rungger is a postdoctoral researcher at the Technical University of Munich and is affiliated with the Hybrid Control Systems Group in the Department of Electrical and Computer Engineering. His research interests lie in the broad area of formal methods in control, including analysis and control of cyber-physical systems and abstraction-based controller design. He received his Dr.-Ing. (PhD) in 2011 from the University of Kassel and the Dipl.-Ing. (MSc) in Electrical Engineering in 2007 from the Technical University of Munich.