Safety control, a quantitative approach

Alina Eqtami, Antoine Girard

Safety control, a quantitative approach ⋆

Alina Eqtami * **Antoine Girard** *

* *Laboratoire des Signaux et Systèmes (L2S)*
CNRS, CentraleSupélec, Université Paris-Sud, Université Paris-Saclay
3, rue Joliot-Curie, 91192 Gif-sur-Yvette, cedex, France
(e-mail: {alina.eqtami,antoine.girard}@l2s.centralesupelec.fr)

Abstract: Safety control consists in maintaining the state of a given system inside a specified set of safe states. Traditionally, the problem is tackled using set-theoretic methods, which are mostly qualitative: states are partitioned between safety-controllable (i.e. states that belong to the maximal controlled invariant subset of the safe set) and safety-uncontrollable states. In this paper, we present a quantitative approach to safety controller synthesis. Our approach makes it possible to compute a measure of safety, which quantifies how far from the unsafe set (respectively, how close to the safe set) one can stay when starting from a given controllable (respectively, uncontrollable) state. For finite transition systems, such a measure can be computed in finite-time using a functional fixed-point iteration. In addition, we show that the level sets of the functional fixed-point coincide with the maximal controlled invariant subsets of a parameterized family of sets and that one can synthesize a common safety controller for all the sets of the family. In the second part of the paper, we show how the approach can be used in the framework of abstraction-based synthesis to lift these results to infinite transition systems with finite abstractions. To illustrate the effectiveness of the approach, we show an application of the approach to a simple boost DC-DC converter.

Keywords: Safety, controlled invariant sets, transition systems, abstraction, quantitative synthesis.

1. INTRODUCTION

In system design, safety refers to the ability of a controller to maintain the state of a system in a specified set of safe states (see e.g. Tabuada (2009); Girard (2012)). The classical approach to safety synthesis is based on the notion of controlled-invariant sets (see e.g. Blanchini and Miani (2008); Maler (2002); Rungger and Tabuada (2017)), where states are said to be safety-controllable, or infinite-time reachable (as in Bertsekas (1972)), if they belong to the maximal controlled-invariant subset of the safe set. This approach is therefore mostly qualitative (states are either safety-controllable or safety-uncontrollable) and does not allow to compare to states within the same category. However, intuitively, some states can be considered as safer than the others (i.e. those that are further from the unsafe set). Similarly, between two unsafe states, the one, which is closer to the safe set, would tend to be more desirable. Hence, it appears natural to take a quantitative approach where a measure of safety is associated to the states of the system.

Such quantitative semantics of qualitative specifications, typically formulated in temporal logic have been given in (Fainekos and Pappas (2009); Donzé and Maler (2010)). Intuitively, these semantics measure how much a trajectory can be perturbed before changing the qualitative value (true or false) of a given property. Hence, for safety properties, these quantitative semantics can be interpreted as follows: for safe trajectories, it measures the minimal distance of the trajectory to the unsafe set; for unsafe trajectories, it measures the maximal distance of the trajectory to the safe set. Quantitative semantics of temporal logic have been used within the model predictive control framework to synthesize receding horizon controllers (Raman et al. (2015); Sadraddini and Belta (2015)).

In this work, we propose a quantitative approach to safety control, based on a functional fixed-point iteration. Convergence of the fixed-point in finite-time is guaranteed for finite transition systems. The level sets of the fixed-point coincide with the maximal controlled invariant subsets of a family of sets parameterized by their distance to the safe set. This allows us to interpret the value of the fixed-point at a given state as a measure of the safety of that state. Moreover, we show that a common safety controller can be synthesized for the whole family of controlled invariant sets. A similar functional fixed-point iteration can be found in (Chatterjee and Henzinger (2008)), however, the characterization of the level sets in terms maximal controlled-invariant sets and results on controller synthesis appear to be new. A second contribution of the paper is the joint use of the quantitative approach with abstraction-based techniques (see e.g. Tabuada (2009); Girard (2012)), which allow us to lift the results from finite transition systems to infinite transition systems with finite abstractions. Let us remark that abstraction-based synthesis of safety controllers with quantitative objectives has also been studied in (Meyer et al. (2015, 2017)). However, in those works, the quantitative objective is an auxiliary performance cost, which is not directly related to the safety property.

The paper is organized as follows. In Section 2, we introduce the class of transition systems and provide a quick overview

⋆ This research was partially supported by Labex DigiCosme (project ANR-11-LABEX-0045-DIGICOSME) operated by ANR as part of the program "Investissement d'Avenir" Idex Paris Saclay (ANR-11-IDEX-0003-02). This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 725144).

of the qualitative approach to the safety control problem. In Section 3, we introduce the quantitative approach to safety control for finite transition systems. In Section 4, we extend the approach to infinite transition systems using abstraction-based techniques. Finally, in Section 5, we show the effectiveness of the approach by appyling it to a simple boost DC-DC converter model.

Notation. In the following, $\mathbb{R}$, $\mathbb{R}_0^+$ and $\mathbb{N}$ denote the set of real, nonnegative real and natural numbers, respectively. A relation $R \subseteq X \times Y$ is identified with the set-valued map $R : X \to 2^Y$ where $R(x) = \{y \in Y | \ (x,y) \in R\}$. The inverse relation of R is $R^{-1} = \{(y,x) \in Y \times X | \ (x,y) \in R\}$. The domain of R is $\mathrm{dom}(R) = \{x \in X | \ R(x) \neq \emptyset\}$.

2. PRELIMINARIES

In this section, we introduce some concepts which will be helpful for the rest of the paper. First, the general modeling framework of transition systems is given and then, some concepts related to safety control are going to be discussed.

2.1 Transition systems

A common modeling framework for discrete, continuous and hybrid systems are the transition systems (see e.g. Tabuada (2009)), that are defined as follows:

Definition 1. A *transition system* T is a quintuple

$$T = (X, U, \Delta, Y, H)$$

consisting of a set of states X; a set of inputs U; a transition relation $\Delta \subseteq X \times U \times X$; a set of observations Y and an output map $H : X \to Y$.

The transition relation captures the dynamics of the transition system and $(x,u,x') \in \Delta$, which will be denoted hereafter as $x' \in \Delta(x,u)$, signifies that the state x' can be reached initiating from x under the control input u. The set of *enabled inputs* at state x is given by $\mathrm{enab}_\Delta(x) = \{u \in U | \ \Delta(x,u) \neq \emptyset\}$. If $\mathrm{enab}_\Delta(x) = \emptyset$, then x is said to be a *blocking* state, otherwise it is said to be *non-blocking*; the set of non-blocking states is denoted nbs_Δ. A transition system is called *finite* if the state and input sets X and U are finite sets, whereas a transition system that is not finite is called *infinite*. A transition system is called *metric* if the output set Y is equipped with a metric d.

In the framework of transition systems, (static state-feedback) controllers can be defined as follows:

Definition 2. A *controller* for the transition system T is a map $C : X \to 2^U$ such that $C(x) \subseteq \mathrm{enab}_\Delta(x)$, for all $x \in X$. The controlled transition system T_C is defined as $T_C = (X, U, \Delta_C, Y, H)$ where the transition relation is given by:

$$x' \in \Delta_C(x,u) \iff [(u \in C(x)) \wedge (x' \in \Delta(x,u))].$$

Note that a state x of the controlled system T_C is non-blocking if and only if $C(x) \neq \emptyset$, i.e. $\mathrm{nbs}_{\Delta_C} = \mathrm{dom}(C)$.

2.2 Safety specifications

Let us consider a transition system T and $X_s \subseteq X$ a set of safe states. In practice, X_s can often be defined from a set of safe outputs $Y_s \subseteq Y$ by $X_s = H^{-1}(Y_s)$.

The problem considered in this paper, known as safety problem in computer science, is traditionally referred to as controlled invariance in control theory. The main objective in safety problems is to characterize a subset of safe states $S \subseteq X_s$, such that when the system's state is initially in S, it can remain in S (and thus in X_s) forever under suitable control. Additionally, one aims at synthesizing a controller which makes it possible to restrict the behavior of a system so that its state remains inside the set S. The definition of controlled invariant subset and the notion of a safety controller are given next.

Definition 3. Let us consider transition system T and $X_s \subseteq X$ a set of safe states:

- $S \subseteq X_s$ is a *controlled invariant subset* of X_s if and only if for all $x \in S$, there exists $u \in \mathrm{enab}_\Delta(x)$ such that $\Delta(x,u) \subseteq S$.
- $S^\star \subseteq X_s$ is the *maximal controlled invariant subset* of X_s if and only if $S^\star$ is a controlled invariant subset of X_s and for all controlled invariant subsets $S \subseteq X_s$, we have $S \subseteq S^\star$.

Notice that the uniqueness of the maximal controlled invariant subset is a well-known result, see e.g. (Ramadge and Wonham (1987)). Algorithms for computing the maximal controlled invariant subset are typically based on fixed-point iteration on sets, see e.g. (Bertsekas (1972); Maler (2002); Rungger and Tabuada (2017)). A state $x \in X$ is said to be *safety-controllable* if $x \in S^\star$; otherwise, it is said to be *safety-uncontrollable*.

Given a controlled invariant subset $S \subseteq X_s$, a safety controller maintains the state of the system T_C inside S:

Definition 4. Let us consider transition system T and $X_s \subseteq X$ a set of safe states, let $S \subseteq X_s$ be a controlled invariant subset of X_s. The controller $C : X \to 2^U$ is a *safety controller* for controlled invariant subset S if, $S \subseteq \mathrm{dom}(C)$ and for all $x \in S$, for all $u \in C(x)$, we have $\Delta(x,u) \subseteq S$.

Given a controlled invariant subset $S \subseteq X_s$, it is always possible to obtain a safety controller C as follows:

$$C(x) := \begin{cases} \emptyset & \text{if } x \notin S \\ \{u \in \mathrm{enab}_\Delta(x) | \ \Delta(x,u) \subseteq S\} & \text{if } x \in S \end{cases} \quad (1)$$

3. QUANTITATIVE APPROACH TO SAFETY CONTROLLER SYNTHESIS

The approach to the safety problem presented in the previous section can be referred to as qualitative, in the sense that the states of T can be partitioned in two categories: the safety controllable states (i.e. $x \in S^\star$) and the safety uncontrollable states (i.e. $x \notin S^\star$). However, for states within a given category, the previous approach does not allow to make a distinction. For instance, given two safety controllable states, one may be interested to know if one is safer than the other; a similar question can be asked for safety uncontrollable states. To answer this question, one needs to take a quantitative approach, i.e. one needs to have a measure of the level of safety is a given state. Intuitively, for a safety controllable state, this measure should quantify how far one can stay from the unsafe set, starting from that state. Conversely, for an safety uncontrollable state, this measure should quantify how close one can stay from the safe set.

The quantitative approach would also be useful for the purpose of controller synthesis. Indeed, controllers obtained by (1) through the qualitative approach have non-deterministic values

for safety controllable states and have an empty value (i.e. are undefined) for safety uncontrollable states. Instead, one could use the quantitative approach to choose the control input that would optimize the level of safety of the corresponding successors.

In this section, we make the assumption that the transition system T is finite. We believe that similar results can be derived for classes of infinite transition systems, but at the expense of more involved technical developments, so the infinite case is left as future work.

To substantiate the quantitative approach to safety controller synthesis, let us introduce a cost function $h : X \to \mathbb{R}$, which intuitively quantifies how safe or unsafe is a given state x. If T is metric, a natural choice for $h(x)$ is the signed distance from the output $H(x)$ to the safe output set Y_s, i.e.

$$h(x) = d_s(H(x), Y_s) \tag{2}$$

with

$$d_s(y, Y_s) = \begin{cases} \sup\{\delta \geq 0 | B(y,\delta) \cap S \neq \emptyset\} & \text{if} \quad y \notin S \\ -\sup\{\delta \geq 0 | B(y,\delta) \subseteq S\} & \text{if} \quad y \in S \end{cases}$$

where $B(y,\delta) = \{y' \in Y |\, d(y,y') \leq \delta\}$ denotes the ball centered in y of radius δ. A positive value of $h(x)$ means that $H(x)$ lies outside the safe output set Y_s: the larger $h(x)$, the further $H(x)$ from Y_s and thus the more unsafe x. Conversely, a negative value of $h(x)$ means that $H(x)$ is inside Y_s: the smaller $h(x)$, the further $H(x)$ from the boundary of Y_s and thus the safer x.

Then, let us define the sequence $(V^k)_{k\in\mathbb{N}}$, where the maps $V^k : X \to \mathbb{R} \cup \{+\infty\}$ are given iteratively as follows. For $k = 0$, and $x \in X$, let $V^0(x) := h(x)$. Then, for every subsequent step, with $k \in \mathbb{N}$ and $x \in X$, let

$$V^{k+1}(x) := \tag{3}$$
$$\begin{cases} \max\left(h(x), \min\limits_{u\in \mathrm{enab}_\Delta(x)} \max\limits_{x'\in\Delta(x,u)} V^k(x')\right) & \text{if} \quad x \in \mathrm{nbs}_\Delta \\ +\infty & \text{if} \quad x \notin \mathrm{nbs}_\Delta \end{cases}$$

The fixed-point is obtained by taking the limit of the sequence:

$$V^\star(x) := \lim_{k\to+\infty} V^k(x). \tag{4}$$

For finite state systems, one can show that the fixed-point is actually reached in a finite number of steps:

Proposition 5. Let T be finite, then the limit (4) exists and there exists $k^\star \in \mathbb{N}$ such that for all $k \geq k^\star$, for all $x \in X$, $V^k(x) = V^{k^\star}(x) = V^\star(x)$. Moreover, $V^\star$ satisfies the following fixed-point equation, for all $x \in \mathrm{nbs}_\Delta$,

$$V^\star(x) = \max\left(h(x), \min_{u\in \mathrm{enab}_\Delta(x)} \max_{x'\in\Delta(x,u)} V^\star(x')\right). \tag{5}$$

Proof. First, we are going to prove that for all $x \in X$, the sequence $(V^k(x))_{k\in\mathbb{N}}$ is nondecreasing. This is obviously the case if $x \notin \mathrm{nbs}_\Delta$. When $x \in \mathrm{nbs}_\Delta$, we have the following

$$V^0(x) = h(x)$$
$$V^1(x) = \max\left(h(x), \min_{u\in \mathrm{enab}_\Delta(x)} \max_{x'\in\Delta(x,u)} V^0(x')\right) \geq V^0(x)$$

Assume now, that for some $k \geq 1$, $V^k(x) \geq V^{k-1}(x)$ for all $x \in X$. Then, for all $x \in \mathrm{nbs}_\Delta$,

$$V^{k+1}(x) = \max\left(h(x), \min_{u\in \mathrm{enab}_\Delta(x)} \max_{x'\in\Delta(x,u)} V^k(x')\right)$$
$$\geq \max\left(h(x), \min_{u\in \mathrm{enab}_\Delta(x)} \max_{x'\in\Delta(x,u)} V^{k-1}(x')\right) = V^k(x)$$

Note that for all $x \notin \mathrm{nbs}_\Delta$, we also have $V^{k+1}(x) \geq V^k(x)$. Thus, by induction, it follows that for all $k \in \mathbb{N}$, for all $x \in X$, we have $V^{k+1}(x) \geq V^k(x)$, i.e. the sequence $(V^k(x))_{k\in\mathbb{N}}$ is nondecreasing. A nondecreasing sequence converges to the supremum of its range. Thus, the limit (4) exists.

To show that the fixed point is reached in a finite number of steps, let us remark that for all $x \in X$, for all $k \in \mathbb{N}$, $V^k(x) \in h(X) \cup \{+\infty\}$, which is finite from the finiteness of X. Hence, for all $x \in X$, $(V^k(x))_{k\in\mathbb{N}}$ is nondecreasing with values in a finite set, which implies that there exists $k_x \in \mathbb{N}$, such that for all $k \geq k_x$, $V^k(x) = V^{k_x}(x) = V^\star(x)$. Let $k^\star = \max_{x\in X} k_x$, which by finiteness of X is well-defined. Then, for all $x \in X$, for all $k \geq k^\star$, $V^k(x) = V^{k^\star}(x) = V^\star(x)$. Finally, by (3) with $k \geq k^\star$, one gets (5). □

Remark 6. If T was infinite, the previous procedure would need to be amended as follows. The minimum and maximum in (3) should be replaced by infimum and supremum, respectively. While the limit (4) would still exist ($V^k(x)$ would remain nondecreasing), the fixed-point would generally not be reached in a finite number of steps.

The relation of the quantitative approach described above to the qualitative approach is highlighted in the following result:

Theorem 7. Let T be finite, then for all $a \in \mathbb{R}$, $S^a = \{x \in X \mid V^\star(x) \leq a\}$ is the maximal controlled invariant subset of the set $X^a = \{x \in X \mid h(x) \leq a\}$. Let us consider the controller $C^\star$ defined by:

$$C^\star(x) = \begin{cases} \emptyset & \text{if } x \notin \mathrm{nbs}_\Delta \\ \arg\min\limits_{u\in \mathrm{enab}_\Delta(x)} \max\limits_{x'\in\Delta(x,u)} V^\star(x') & \text{if } x \in \mathrm{nbs}_\Delta \end{cases} \tag{6}$$

Then, for all $a \in \mathbb{R}$, $C^\star$ is a safety controller for controlled invariant subset S^a.

Proof. The proof of this Theorem is twofold: (i) firstly we are going to prove that the set S^a is a controlled invariant subset of X^a, and admitting $C^\star$ as an associated safety controller; (ii) secondly, we will show that S^a is the maximal controlled invariant subset X^a.

(i) First, let us remark that $\mathrm{dom}(C^\star) = \mathrm{nbs}_\Delta$. Let $x \in S^a$, since $V^\star(x) \leq a < +\infty$, it follows that $x \in \mathrm{nbs}_\Delta$, thus $S^a \subseteq \mathrm{dom}(C^\star)$. By (5), we have $h(x) \leq V^\star(x) \leq a$ and $x \in X^a$, thus, $S^a \subseteq X^a$. Then, let $u \in C^\star(x)$, and $x' \in \Delta(x,u)$, then by definition of $C^\star$ one gets:

$$V^\star(x') \leq \max_{z'\in\Delta(x,u)} V^\star(z') = \min_{v\in \mathrm{enab}_\Delta(x)} \max_{z'\in\Delta(x,v)} V^\star(z').$$

It then follows from (5) that

$$\min_{v\in \mathrm{enab}_\Delta(x)} \max_{z'\in\Delta(x,u)} V^\star(z') \leq V^\star(x).$$

Therefore, $V^\star(x') \leq V^\star(x) \leq a$ and the set S^a is a controlled invariant subset of X^a and $C^\star$ is an associated safety controller.

(ii) Now, the maximality of S^a is going to be established. Let us consider a controlled invariant subset $S \subseteq X^a$. We need to prove that $S \subseteq S^a$. We have that for all $x \in S$, $V^0(x) = h(x) \leq a$. Assume, now, that for some $k \in \mathbb{N}$, for all $x \in S$, $V^k(x) \leq a$. Let $x \in S$, then there exists $u \in \mathrm{enab}_\Delta(x)$ such that $\Delta(x,u) \subseteq S$. Hence, for all $x' \in \Delta(x,u)$, $V^k(x') \leq a$. This implies that

$$\min_{u\in \mathrm{enab}_\Delta(x)} \max_{x'\in\Delta(x,u)} V^k(x') \leq a.$$

Moreover, since $h(x) \leq a$, it follows from (3) that

$$V^{k+1}(x) = \max\left(h(x), \min_{u\in \mathrm{enab}_\Delta(x)} \max_{x'\in\Delta(x,u)} V^k(x')\right) \leq a.$$

By induction, we obtain that for all $x \in S$, for all $k \in \mathbb{N}$, $V^k(x) \leq a$. Taking the limit, we obtain $V^\star(x) \leq a$ for all $x \in S$ and thus $S \subseteq S^a$. $\square$

The advantages of the quantitative approach over the qualitative approach are clear from Theorem 7. Firstly, the quantitative approach allows us to compute, using a single fixed point iteration, the maximal controlled invariant subsets of a parameterized family of safe sets. To do the same thing, the qualitative approach would require to proceed with one fixed-point iteration for each value of the parameter. Secondly, while the qualitative approach, using (1), would synthesize one different safety controller for each maximal controlled invariant subsets of the parameterized family, the quantitative approach allows us to design a common safety controller $C^\star$ given by (6), for the whole family of maximal controlled invariant subsets.

We can see from (6), that $C^\star$ chooses inputs that will minimize the (worst-case) value of $V^\star$ at the next state. It is remarkable that using controller $C^\star$, the function $V^\star$ acts as a weak Lyapunov function (i.e. it is non-increasing) along the trajectories of the controlled system $T_{C^\star}$. Then, the value $V^\star(x)$ provides a measure of the level of safety of x, since the value of $V^\star$ and thus of h along trajectories of $T_{C^\star}$ starting from state x remains smaller than or equal to $V^\star(x)$. If x is safety uncontrollable, then $V^\star(x) > 0$, and the outputs of trajectories starting from x remain at a distance from Y_s smaller than or equal to $V^\star(x)$. If x is safety controllable, then $V^\star(x) < 0$, and the outputs of trajectories starting from x remain at a distance from the unsafe set $Y \setminus Y_s$ greater than or equal to $-V^\star(x)$.

4. ABSTRACTION-BASED SYNTHESIS USING THE QUANTITATIVE APPROACH

In this section, we show how the quantitative approach can be used in the context of abstraction-based synthesis.

4.1 Approximate alternating simulation and bisimulation

Abstraction-based synthesis requires the use of formal behavioral relationships between transition systems. In the following, T_1 denotes a finite abstraction while T_2 denotes the concrete (possibly infinite) system. We consider transition systems formally related by approximate alternating simulation relations (Tabuada (2009)) defined as follows:

Definition 8. Let $T_i = (X_i, U_i, \Delta_i, Y, H_i)$ with $i = 1,2$, be two metric transition systems with the same set of outputs Y and let $\delta \in \mathbb{R}_0^+$. A relation $R \subseteq X_1 \times X_2$ is a *δ-approximate alternating simulation* relation from T_1 to T_2 if the following are satisfied:

(1) For every $x_1 \in X_1$ there exists $x_2 \in X_2$ with $(x_1, x_2) \in R$;
(2) for every $(x_1, x_2) \in R$ we have $d(H_1(x_1), H_2(x_2)) \leq \delta$;
(3) for every $(x_1, x_2) \in R$ and for every $u_1 \in \text{enab}_{\Delta_1}(x_1)$ there exists $u_2 \in \text{enab}_{\Delta_2}(x_2)$ such that for every $x_2' \in \Delta_2(x_2, u_2)$ there exists $x_1' \in \Delta(x_1, u_1)$ satisfying $(x_1', x_2') \in R$

We say that T_1 is δ-approximately alternatingly simulated by T_2, denoted by $T_1 \preceq^\delta T_2$ if there exists a δ-approximate alternating simulation relation from T_1 to T_2.

Accordingly, we can define the approximate alternating bisimulation relations (Tabuada (2009)) as follows:

Definition 9. Let $T_i = (X_i, U_i, \Delta_i, Y, H_i)$ with $i = 1,2$, be two metric transition systems with the same set of outputs Y and let $\delta \in \mathbb{R}_0^+$. A relation $R \subseteq X_1 \times X_2$ is said to be a *δ-approximate alternating bisimulation* relation between T_1 to T_2 if the following are satisfied:

(1) R is a δ-approximate alternating simulation relation from T_1 to T_2;
(2) R^{-1} is a δ-approximate alternating simulation relation from T_2 to T_1.

We say that T_1 is δ-approximately alternatingly bisimilar to T_2, denoted by $T_1 \sim^\delta T_2$, if there exists a δ-approximate alternating bisimulation relation between T_1 and T_2.

4.2 Abstraction-based synthesis

In this section, we show how the use of the quantitative approach on a discrete abstraction makes it possible to obtain a parameterized family of controlled invariant subsets for the concrete system.

Theorem 10. Let T_i with $i = 1,2$, be two metric transition systems with the same set of outputs Y such that $T_1 \preceq^\delta T_2$ with δ-approximate alternating simulation relation R. Let $Y_s \subseteq Y$ be a subset of safe outputs and h_i be given by (2) with $i = 1,2$. Let us assume T_1 is finite and let $V_1^\star$ and $C_1^\star$ be accordingly given by (4) and (6). For $a \in \mathbb{R}$, let $S_1^a = \{x_1 \in X_1 |\ V_1^\star(x_1) \leq a\}$, then

- $\tilde{S}_2^a = R(S_1^a)$ is a controlled-invariant subset of $X_2^{a+\delta} = \{x_2 \in X_2 |\ h_2(x_2) \leq a + \delta\}$.
- A safety controller for $\tilde{S}_2^a$ is given for all $x_2 \in X_2$ by

$$C_2^a(x_2) = \left\{ u_2 \in \text{enab}_{\Delta_2}(x_2) \;\middle|\; \begin{array}{c} \exists x_1 \in R^{-1}(x_2) \cap S_1^a, \\ \exists u_1 \in C_1^\star(x_1), \\ \Delta_2(x_2, u_2) \subseteq R(\Delta_1(x_1, u_1)) \end{array} \right\} \tag{7}$$

Proof. We first prove that $\tilde{S}_2^a$ is a subset of $X_2^{a+\delta}$. For all $x_2 \in \tilde{S}_2^a$, there exists $x_1 \in S_1^a$ such that $(x_1, x_2) \in R$. From Definition 8, we have $d(H_1(x_1), H_2(x_2)) \leq \delta$. From Theorem 7, S_1^a is a subset of $X_1^a = \{x_1 \in X_1 |\ h_1(x_1) \leq a\}$. Since h_i are given by (2) with $i = 1,2$, it follows from the triangular inequality that

$$h_2(x_2) \leq h_1(x_1) + d(H_1(x_1), H_2(x_2)) \leq a + \delta.$$

Hence $x_2 \in X_2^{a+\delta}$.

We now prove that $\tilde{S}_2^a$ is a controlled invariant subset admitting C_2^a as safety controller. We first prove that $\tilde{S}_2^a \subseteq \text{dom}(C_2^a)$. Let $x_2 \in \tilde{S}_2^a$ then there exists $x_1 \in S_1^a$ such that $(x_1, x_2) \in R$. From Theorem 7, S_1^a is a controlled invariant subset with $C_1^\star$ as associated safety controller. Hence $x_1 \in S_1^a \subseteq \text{dom}(C_1^\star)$. Then, let $u_1 \in C_1^\star(x_1)$, from Definition 8, there exists $u_2 \in \text{enab}_{\Delta_2}(x_2)$ such that $\Delta_2(x_2, u_2) \subseteq R(\Delta_1(x_1, u_1))$. It follows from (7) that $u_2 \in C_2^a(x_2)$ and thus $x_2 \in \text{dom}(C_2^a)$.

Now, let $x_2 \in \tilde{S}_2^a$, and $u_2^a \in C_2^a(x_2)$, then from (7) there exists $x_1 \in R^{-1}(x_2) \cap S_1^a$ and $u_1 \in C_1^\star(x_1)$ such that $\Delta_2(x_2, u_2) \subseteq R(\Delta_1(x_1, u_1))$. Since $x_1 \in S_1^a$ and $u_1 \in C_1^\star(x_1)$, it follows from Theorem 7, that $\Delta_1(x_1, u_1) \subseteq S_1^a$. Hence, $\Delta_2(x_2, u_2) \subseteq R(S_1^a) = \tilde{S}_2^a$. Hence $\tilde{S}_2^a$ is a controlled invariant subset and C_2^a is an associated safety controller. $\square$

One can see from (7) that the controller C_2^a generally depends on the value of the parameter a, while the controller $C_1^\star$ for the abstraction does not and is common for all controlled-invariant subset S_1^a, $a \in \mathbb{R}$. For the concrete system, a common safety

controller for all controlled-invariant subset $\tilde{S}_2^a$, $a \in \mathbb{R}$, can be obtained as follows:

Corollary 11. Under the assumptions of Theorem 10, a common safety controller for $\tilde{S}_2^a$, $a \in \mathbb{R}$ is given for all $x_2 \in X_2$ by

$$C_2(x_2) = \left\{ u_2 \in \mathrm{enab}_{\Delta_2}(x_2) \;\middle|\; \begin{array}{c} \exists x_1 \in \arg \min\limits_{z_1 \in R^{-1}(x_2)} V_1^\star(z_1), \\ \exists u_1 \in C_1^\star(x_1), \\ \Delta_2(x_2,u_2) \subseteq R(\Delta_1(x_1,u_1)) \end{array} \right\} \tag{8}$$

Proof. Let $a \in \mathbb{R}$, let $x_2 \in \tilde{S}_2^a$, and $x_1 \in \arg\min_{z_1 \in R^{-1}(x_2)} V_1^\star(z_1)$. Since $\tilde{S}_2^a = R(S_1^a)$, we have

$$V_1^\star(x_1) = \min_{z_1 \in R^{-1}(x_2)} V_1^\star(z_1) \leq a,$$

which gives that $x_1 \in S_1^a$. Hence, it follows that for all $x_2 \in \tilde{S}_2^a$, $C_2(x_2) \subseteq C_2^a(x_2)$. It then follows from Theorem 10 that C_2 is a safety controller for all $\tilde{S}_2^a$, $a \in \mathbb{R}$, such that $\tilde{S}_2^a \subseteq \mathrm{dom}(C_2)$.

Then, let $x_2 \in \tilde{S}_2^a$ and $x_1 \in \arg\min_{z_1 \in R^{-1}(x_2)} V_1^\star(z_1)$, from above we have $x_1 \in S_1^a \subseteq \mathrm{dom}(C_1^\star)$. Then, let $u_1 \in C_1^\star(x_1)$, from Definition 8, there exists $u_2 \in \mathrm{enab}_{\Delta_2}(x_2)$ such that $\Delta_2(x_2,u_2) \subseteq R(\Delta_1(x_1,u_1))$. It follows from (8) that $u_2 \in C_2(x_2)$ and thus $x_2 \in \mathrm{dom}(C_2)$. Hence $\tilde{S}_2^a \subseteq \mathrm{dom}(C_2)$. □

When both transition systems T_1 and T_2 are finite, the following result makes it possible to compare the functions $V_1^\star$ and $V_2^\star$:

Theorem 12. Let T_i with $i = 1,2$, be two metric transition systems with the same set of outputs Y. Let $Y_s \subseteq Y$ be a subset of safe outputs and h_i be given by (2) with $i = 1,2$. Let us assume T_1 and T_2 are finite and let $V_1^\star$ and $V_2^\star$ be accordingly given by (4). Then,

- If $T_1 \preceq^\delta T_2$, with δ-approximate alternating simulation relation R, we have
$$\forall (x_1,x_2) \in R,\ V_2^\star(x_2) \leq V_1^\star(x_1) + \delta.$$
- If $T_1 \sim^\delta T_2$, with δ-approximate alternating bisimulation relation R, we have
$$\forall (x_1,x_2) \in R,\ V_1^\star(x_1) - \delta \leq V_2^\star(x_2) \leq V_1^\star(x_1) + \delta.$$

Proof. We prove the first item. Let $(x_1,x_2) \in R$, let $a = V_1^\star(x_1)$ and let $S_1^a = \{z_1 \in X_1 |\ V_1^\star(z_1) \leq a\}$. Clearly, $x_1 \in S_1^a$ and therefore $x_2 \in \tilde{S}_2^a = R(S_1^a)$. From Theorem 10, we have that $\tilde{S}_2^a$ is a controlled invariant subset of $X_2^{a+\delta}$. By Theorem 7, $S_2^{a+\delta} = \{z_2 \in X_2 |\ V_2^\star(z_2) \leq a+\delta\}$ is the maximal controlled invariant subset of $X_2^{a+\delta}$. Thus, $\tilde{S}_2^a \subseteq S_2^{a+\delta}$. It follows that $V_2^\star(x_2) \leq a+\delta = V_1^\star(x_1) + \delta$.

We now prove the second item. $T_1 \sim^\delta T_2$ implies that R is a δ-approximate alternating simulation relation from T_1 to T_2. Then, it results from the above that, for all $(x_1,x_2) \in R$, $V_2^\star(x_2) \leq V_1^\star(x_1) + \delta$. R^{-1} is also a δ-approximate alternating simulation relation from T_2 to T_1. Then, for all $(x_1,x_2) \in R$, $V_1^\star(x_1) \leq V_2^\star(x_2) + \delta$. □

5. NUMERICAL RESULTS

In this section, we illustrate the results presented in the previous sections using the boost DC-DC converter. This electric power convertor has two operation modes depending on the position of a switch. It can be modeled as a switched system with two modes and the two dimensional dynamics associated with both modes are affine of the form:

$$\dot{x}(t) = A_{p(t)}x(t) + b$$

with $p(t) \in \{1,2\}$ and $x(t) \in \mathbb{R}^2$. For numerical values of the system matrices, see (Girard et al. (2010)).

We sample time with period $\tau = 0.5$ and represent the sampled dynamics of the switched system as an infinite transition system T_2. Following the approach described in (Girard et al. (2010)), one can compute δ-approximately (alternatingly) bisimilar discrete abstractions for arbitrary precision $\delta > 0$. Choosing $\delta = 0.2$ and restricting the dynamics of the abstraction to the compact set $X = [0.65,1.65] \times [4.95,5.95]$, one obtains a finite abstraction T_1 with 264196 states. Note that in this approach, there is no distinction between states and outputs (i.e. the output map is the identity map).

We consider the safety control problem, which consists in maintaining the state of the system within the set $X_S = Y_S = [1.1,1.6] \times [5.4,5.9]$. Using the finite abstraction, we apply the functional fixed-point algorithm (3), which terminates after 107 iterations. The fixed-point $V_1^\star$ is shown in Figure 1, while

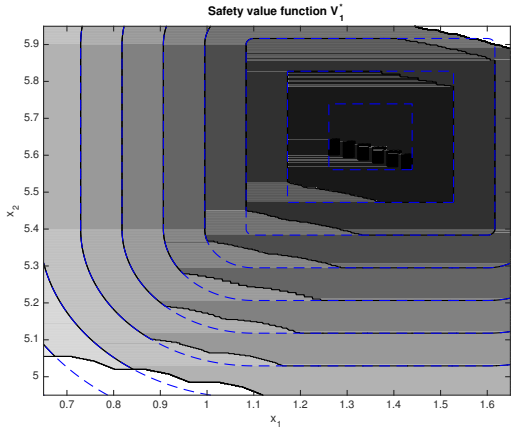

Fig. 1. Fixed-point $V_1^\star$ of algorithm (3) for the boost DC-DC converter. The dashed blue lines depict different level sets X_1^a of the function h_1 for different values of the parameter $a \in \mathbb{R}$. Gray colors depict different level sets S_1^a of the function $V_1^\star$ for the same values of a; white color correspond to states x_1 such that $V_1^\star(x_1) = +\infty$.

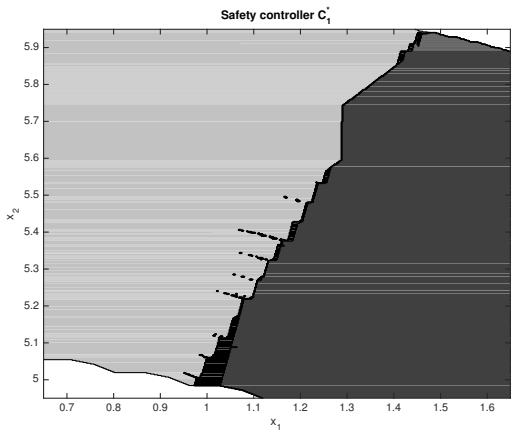

Fig. 2. Safety controller $C_1^\star$ for the boost DC-DC converter. Light gray: mode 1, dark gray: mode 2, black: both modes are enabled, white: blocking states.

the resulting safety controller $C_1^\star$ given by (6) is shown on Fig.2. In particular, one can see that $V_1^\star$ characterizes maximal controlled-invariant subsets of a family of sets parameterized by their distance to the safe set. Remarkably, the controller $C_1^\star$ is a common safety controller for all these controlled-invariant subsets.

On Figure 3, one can check that $V_1^\star$ acts as a weak Lyapunov function (i.e. it is non-increasing) for the controlled transition system $T_{1C_1^\star}$, where we used a lazy implementation of the controller $C_1^\star$: when there is a choice between mode 1 and 2, the controller selects the one that is already on. Figure 4 shows a trajectory of the concrete system T_2 (i.e. the switched system), associated to the trajectory of the controlled abstraction $T_{1C_1^\star}$ depicted in Figure 3. It can be witnessed that the trajectory never goes beyond the safe set, which is represented by the green dashed lines in the figure. Moreover, the controller tends to keep to trajectory away from the boundary of the safe set.

6. CONCLUSION

In this paper, we have presented a quantitative approach to safety controller synthesis. We have shown how using a functional fixed-point iteration, one can compute a measure of safety of the sates of a finite transition system. The measure also provides a simple design for a safety controller that is common to a family of parameterized controlled-invariant sets. Using abstraction-based techniques, we have shown that the approach can be lifted to infinite transition systems. A numerical example shows the effectiveness of the approach.

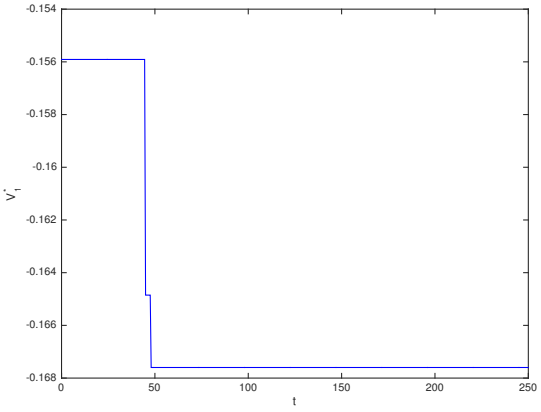

Fig. 3. Time evolution of the function $V_1^\star$ along a trajectory of the controlled abstraction $T_{1C_1^\star}$.

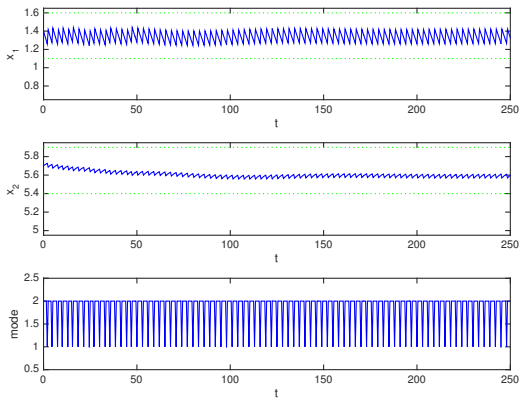

Fig. 4. Trajectory of the concrete system T_2, associated to the trajectory of the controlled abstraction $T_{1C_1^\star}$ depicted in Figure 3. From up to bottom: in blue, time evolution of the state components and inputs; the dashed green lines represent the safe set.

This work opens many further research directions. The most immediate extension of the work is to adapt the theoretical results to generalize the functional fixed-point iteration to a class of infinite transition systems. Secondly, similar quantitative controller synthesis approaches should be developed for other types of specifications such as reachability, stability or more complex properties expressed in some temporal logic. Thirdly, an intriguing question is to investigate the relation between quantitative synthesis and the synthesis of robust controllers for qualitative specifications.

REFERENCES

Bertsekas, D. (1972). Infinite time reachability of state-space regions by using feedback control. *IEEE Transactions on Automatic Control*, 17(5), 604–613.

Blanchini, F. and Miani, S. (2008). *Set-theoretic methods in control*. Springer.

Chatterjee, K. and Henzinger, T.A. (2008). Value iteration. In *25 Years of Model Checking*, 107–138. Springer.

Donzé, A. and Maler, O. (2010). Robust satisfaction of temporal logic over real-valued signals. In *International Conference on Formal Modeling and Analysis of Timed Systems*, 92–106. Springer.

Fainekos, G.E. and Pappas, G.J. (2009). Robustness of temporal logic specifications for continuous-time signals. *Theoretical Computer Science*, 410(42), 4262–4291.

Girard, A. (2012). Controller synthesis for safety and reachability via approximate bisimulation. *Automatica*, 48(5), 947 – 953.

Girard, A., Pola, G., and Tabuada, P. (2010). Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Transactions on Automatic Control*, 55(1), 116–126.

Maler, O. (2002). Control from computer science. *Annual Reviews in Control*, 26(2), 175–187.

Meyer, P.J., Rungger, M., Luttenberger, M., Esparza, J., and Zamani, M. (2017). Quantitative implementation strategies for safety controllers. *arXiv preprint arXiv:1712.05278*.

Meyer, P.J., Girard, A., and Witrant, E. (2015). Safety control with performance guarantees of cooperative systems using compositional abstractions. *IFAC-PapersOnLine*, 48(27), 317–322.

Ramadge, P.J. and Wonham, W.M. (1987). Modular feedback logic for discrete event systems. *SIAM Journal on Control and Optimization*, 25(5), 1202 – 1218.

Raman, V., Donzé, A., Sadigh, D., Murray, R.M., and Seshia, S.A. (2015). Reactive synthesis from signal temporal logic specifications. In *International Conference on Hybrid Systems: Computation and Control*, 239–248. ACM.

Rungger, M. and Tabuada, P. (2017). Computing robust controlled invariant sets of linear systems. *IEEE Transactions on Automatic Control*, 62(7), 3665–3670.

Sadraddini, S. and Belta, C. (2015). Robust temporal logic model predictive control. In *Annual Allerton Conference on Communication, Control, and Computing*, 772–779. IEEE.

Tabuada, P. (2009). *Verification and Control of Hybrid Systems: A Symbolic Approach*. Springer US.