Guaranteed Control of Sampled Switched Systems using Semi-Lagrangian Schemes and One-Sided Lipschitz Constants

Adrien Le Coënt, Laurent Fribourg

Guaranteed Control of Sampled Switched Systems using Semi-Lagrangian Schemes and One-Sided Lipschitz Constants

Adrien Le Coënt[1] and Laurent Fribourg[2]

***Abstract*— In this paper, we propose a new method for ensuring formally that a controlled trajectory stay inside a given safety set $\mathcal{S}$ for a given duration T. Using a finite gridding $\mathcal{X}$ of $\mathcal{S}$, we first synthesize, for a subset of initial nodes x of $\mathcal{X}$, an *admissible control* for which the Euler-based *approximate trajectories* lie in $\mathcal{S}$ at $t \in [0,T]$. We then give sufficient conditions which ensure that the *exact trajectories*, under the same control, also lie in $\mathcal{S}$ for $t \in [0,T]$, when starting at initial points "close" to nodes x. The statement of such conditions relies on results giving estimates of the deviation of Euler-based approximate trajectories, using *one-sided Lipschitz constants*. We illustrate the interest of the method on several examples, including a stochastic one.**

I. Introduction

Consider an ordinary differential equation (ODE) of the form $\dot{z} = f(z)$ on $\mathbb{R}^n$. Classically, one knows that, if the function f is Lipschitz continuous with Lipschitz constant L, the solution of the ODE starting at a given initial value exists and is unique. Besides, one has:

$$\|X_{t,z_1} - X_{t,z_2}\| \leq e^{Lt}\|z_1 - z_2\|, \tag{1}$$

where $\|\cdot\|$ denotes the Euclidean norm, and X_{t,z_i} denotes the value of the solution of the ODE at time t, starting at initial value z_i ($i = 1,2$). This gives a rough *growth bound*, i.e. a function bounding the distance of neighboring trajectories as t evolves.

In the 90's, several researchers [9], [21] have obtained a more accurate growth bound, using the notion of "one-sided Lipschitz (OSL)" function. The function f is said to be OSL if there exists a constant $\lambda \in \mathbb{R}$ such that, for all $z_1, z_2 \in \mathbb{R}^n$:

$$\langle f(z_1) - f(z_2), z_1 - z_2\rangle \leq \lambda\|z_1 - z_2\|^2,$$

where $\langle\cdot,\cdot\rangle$ denotes the scalar product of two vectors of $\mathbb{R}^n$. The real λ is called the OSL constant associated with f. In [9], it is proven that, if f is continuous and OSL with OSL constant λ, then the solution of the ODE starting at a given initial value exists and is unique, and, for all $z_1, z_2 \in \mathbb{R}^n$:

$$\|X_{t,z_1} - X_{t,z_2}\| \leq e^{\lambda t}\|z_1 - z_2\|. \tag{2}$$

This gives a more accurate growth bound because a Lipschitz function f is always OSL, and the associated OSL constant λ is always less than or equal to its Lipschitz counterpart L. Furthermore, in the case of "stiff" differential equations, we have $\lambda \ll L$ (see [9]). Note also that a function can be OSL but not Lipschitz (not even *locally* Lipschitz): inequation (2) then still applies while inequation (1) does not apply any longer. Using the OSL constant λ, it is also possible to bound the error $\|X_{t,z_1} - \tilde{X}_{t,z_2}\|$ in function of $\|z_1 - z_2\|$, where $\tilde{X}_{t,z_2}$ denotes the *Euler approximate* $z_2 + tf(z_2)$ of the solution X_{t,z_2}. In [6], we have derived some analytic forms of such error estimates when one focuses on a compact subdomain $\mathcal{S} \subset \mathbb{R}^n$ of solutions. We have also given an OSL-based error estimate for (a variant of) the Euler-Maruyama approximate solution in the case of *stochastic* ODEs [20]. These results have been used to synthesize controls that are "correct-by-construction", in the sense that they are guaranteed to satisfy given *safety constraints* [6], [20]. In this paper, we show how such error estimates can be integrated to *semi-Lagrangian (SL) schemes* in order to synthesize *optimal* controls for problems with safety constraints.

The plan of the paper is as follows: in Section II, we present the context of our work and the principle of the method; in Section III, we give formal sufficient conditions that guarantee the safety of the control; Section IV illustrates on two examples how the method can be extended for stochastic ODEs and differential games; we conclude in Section V.

II. Context and Principle of the Method

Let us present the context and the principle of our method.

A. Switched systems

A hybrid system is a system where the state evolves continuously according to several possible modes, and where the change of modes (switching) is done instantaneously.We consider here the special case of hybrid systems called "sampled switched systems" [15] where the change of modes occurs periodically with a period of τ seconds. We will suppose furthermore that the state keeps its value when the mode is changed (no jump). More formally, we denote the state of the system at time t by $z(t) \in \mathbb{R}^n$. The set of modes A is *finite*. With each mode $a \in A$ is associated a vector field f_a that governs the state $z(t)$, we have:

$$\dot{z}(t) = f_a(z(t)).$$

We make the following hypothesis:

$(H0)$ For all $a \in A$, f_a is a locally Lipschitz continuous map.

We will denote by X^a_{t,z_0} the solution at time t of $\dot{z}(t) = f_a(z(t))$ with $z(0) = z_0$. The existence of X^a_{t,z_0} is guaranteed by assumption $(H0)$. Let us consider $\mathcal{S} \subset \mathbb{R}^n$ be a

[1]Department of Computer Science, Aalborg University adrien@cs.aau.dk
[2]LSV - ENS Paris-Saclay & CNRS fribourg@lsv.fr

compact and convex set, typically a "rectangular set", i.e. a cartesian product on n closed intervals. We know by $(H0)$ that there exists a constant $L_a > 0$ such that:

$$\|f_a(z_1) - f_a(z_2)\| \leq L_a \|z_1 - z_2\| \quad \forall z_1, z_2 \in \mathcal{S}. \quad (3)$$

We also define, for all $a \in A$:

$$C_a = \sup_{z \in \mathcal{S}} L_a \|f_a(z)\|. \quad (4)$$

Let us denote by $\mathcal{T}$ a compact overapproximation of the set of trajectories starting in $\mathcal{S}$ for $0 \leq t \leq \tau$, i.e. $\mathcal{T}$ is such that

$$\mathcal{T} \supseteq \{X^a_{t,z_0} \mid a \in A, 0 \leq t \leq \tau, z_0 \in \mathcal{S}\}. \quad (5)$$

The existence of $\mathcal{T}$ is guaranteed by assumption $(H0)$. It follows from $(H0)$ that the vector fields f_a of the system are OSL on $\mathcal{T}$: for all $a \in A$, there exists a constant $\lambda_a \in \mathbb{R}$ such that

$$\langle f_a(z_1) - f_a(z_2), z_1 - z_2 \rangle \leq \lambda_a \|z_1 - z_2\|^2 \quad \forall z_1, z_2 \in \mathcal{T}. \quad (6)$$

We consider a *finite time horizon* problem: we suppose that time t belongs to interval $[0, k\tau]$, where k is a given integer number. Given a sequence of modes (or "pattern") $\pi := a_1 \cdots a_k \in A^k$, we denote by X^π_{t,z_0} the solution of the ODE of mode a_1 for $t \in [0, \tau[$ with initial condition z_0, extended continuously with the solution of the ODE of mode a_2 for $t \in [\tau, 2\tau[$, and so on iteratively until mode a_k for $t \in [(k-1)\tau, k\tau]$.

B. Optimal problems

We consider the *cost function*: $J_{k,\tau} : \mathbb{R}^n \times A^k \to \mathbb{R}_{\geq 0}$ defined by:

$$J_{k,\tau}(z_0, \pi) = \|X^\pi_{k\tau,z_0} - z_{ref}\|,$$

and z_{ref} a given "target" state of $\mathbb{R}^n$.

We consider the *value function* $\mathbf{v}^\tau_k : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ defined by:

$$\mathbf{v}^\tau_k(z_0) := \min_{\pi \in A^k} \{J_{k,\tau}(z_0, \pi)\} \equiv \min_{\pi \in A^k} \{\|X^\pi_{k\tau,z_0} - z_{ref}\|\}.$$

The function $\min$ is well-defined because the set A is finite.

We consider the following *finite time horizon optimal control problem*:

Given $k \in \mathbb{N}$ and $\tau \in \mathbb{R}_{>0}$, find for each $z \in \mathbb{R}^n$

- the *value* $\mathbf{v}^\tau_k(z_0)$, i.e.

$$\min_{\pi \in A^k} \{\|X^\pi_{k\tau,z_0} - z_{ref}\|\},$$

- and an *optimal pattern*:

$$\pi^k_\tau(z_0) := arg \min_{\pi \in A^k} \{\|X^\pi_{k\tau,z_0} - z_{ref}\|\}.$$

We are interested here in an optimal problem with *safety constraints*: we want that all the trajectories starting in $\mathcal{S}$ always stay in $\mathcal{S}$ for $t \in [0, k\tau]$. More precisely, we will focus on control patterns $\pi \in A^k$ that are "admissible for $z_0 \in \mathcal{S}$", i.e. such that: $X^\pi_{i\tau,z_0} \in \mathcal{S}$, for all $i \in \{1, \ldots, k\}$ (*discrete-time safety* constraint). We will also consider a stronger admissibility criterion requiring: $X^\pi_{t,z_0} \in \mathcal{S}$, for all $t \in [0, k\tau]$ (*continuous-time safety* constraint).

In order to solve such optimal control problems, it is classical to *spatially discretize* the set $\mathcal{S} \subset \mathbb{R}^n$. Given a hyper-rectangle $\mathcal{S}$, we consider a *partition* of $\mathcal{S}$ into a finite number of hyper-rectangular cells. The *grid* $\mathcal{X}$ associated with $\mathcal{S}$ is the set of all the cell centers. We suppose furthermore that the radius of every cell is upper bounded by a given positive real ε: each cell C of center x is such that $\|z_0 - x\| \leq \varepsilon$, for all $z_0 \in C$. The center $x \in \mathcal{X}$ of a cell $C \subset \mathcal{S}$ is said to be the "ε-representative" of all point of C. Since the set of cells forms a partition of $\mathcal{S}$, each point $z_0 \in \mathcal{S}$ has a unique ε-representative $x \in \mathcal{S}$ with $\|z_0 - x\| \leq \varepsilon$.

In this context, the idea of a Semi-Lagrangian (SL) procedure is the following: we consider the points of $\mathcal{X}$ as the vertices of a finite oriented graph; there is a connection from $x \in \mathcal{X}$ to $x' \in \mathcal{X}$ if x' is the ε-representative of the Euler-based image $(x + \tau f_a(x))$ of x, for some $a \in A$. We then compute using dynamic programming the "path of length k with minimal cost" starting at x: such a path is a sequence of $n+1$ connected points $x\ x_k\ x_{k-1}\ \cdots\ x_1$ of $\mathcal{X}$ which minimises the distance $\|x_1 - z_{ref}\|$. The dynamic progamming procedure thus gives us a *spatially discrete value function* $\mathbf{v}^{\tau,\varepsilon}_k : \mathcal{X} \to \mathbb{R}_{\geq 0}$, and a *spatially discrete pattern function* $\pi^k_{\tau,\varepsilon} : \mathcal{X} \to A^k$ which "approximate" on $\mathcal{S}$ their counterparts $\mathbf{v}^\tau_k$ and π^k_τ respectively.

There is a vast literature on SL-schemes (see, e.g., [7], [12]) which gives numerous results to the following *convergence* problem P1:

"Under which conditions does the spatially-discrete value function $\mathbf{v}^{\tau,\varepsilon}_k$ converge to the value function $\mathbf{v}^\tau_k$ when $\varepsilon \to 0$?"

Actually, when ε decreases too much, the computations with SL-procedures become quickly impractical. We prefer to consider here that ε is *fixed* (as well as τ and k), and focus on the following (local) problem P2:

"Given $z_0 \in \mathcal{S}$, under which conditions does there exist a pattern $\pi \in A^k$ which guarantees:

1) the satisfaction of the safety constraint $X^\pi_{i\tau,z_0} \in S$ for all $i \in \{1, \ldots, k\}$ (or $X^\pi_{t,z_0} \in S$, for all $t \in [0, k\tau]$),
2) while minimizing $\|X^\pi_{k\tau,z_0} - z_{ref}\|$ as much as possible ?"

In order to solve problem P2, we use the SL-based procedure as sketched out above. Given a point $z \in \mathcal{S}$ of ε-representative $x \in \mathcal{X}$, we apply the SL procedure to x. The procedure generates a path of the form $x\ x_k\ x_{k-1}\ \cdots\ x_1$, where $x_k, \cdots, x_1$ are computed using an *Euler scheme*, and lie by construction in $\mathcal{S}$. The associated control pattern is of the form $a_k\ a_{k-1}\cdots a_1 \in A^k$. Let $\pi_i := a_k \cdots a_i$ for $1 \le i \le k$. In order, to ensure that the corresponding points $X^{\pi_1}_{\tau,z}, X^{\pi_2}_{2\tau,z}, \ldots X^{\pi_k}_{k\tau,z}$ of the *exact trajectory* lie also in $\mathcal{S}$, we need to establish a bound on the pairwise distances:

$$\|x - z_0\|,\ \|x_k - X^{\pi_1}_{\tau,z_0}\|,\ \|x_{k-1} - X^{\pi_2}_{2\tau,z_0}\|,\ \ldots,\ \|x_i - X^{\pi_i}_{(k-i+1)\tau,z_0}\|,\ \ldots,\ \|x_1 - X^{\pi_k}_{k\tau,z_0}\|.$$

At time $t = 0$, the first distance $\|x - z_0\|$ is known to be bounded by ε. We will establish bounds $\Delta_1, \ldots, \Delta_k$ on the following distances using a recent result which gives an upper bound to the deviation of Euler-based trajectories with time (see [6]). More precisely, we will give an error function $\Delta(t)$ measuring the distance at time t between an approximate (Euler-based) trajectory starting at $x \in \mathcal{X}$ given by the SL-scheme, and an exact trajectory starting from the cell of x. In order to guarantee that the exact trajectory always lies in the hypercube $\mathcal{S}$ at times $t = \tau, 2\tau, \ldots, k\tau$, we merely perform two simple operations:

1) compute the "safety margin" of the Euler-based trajectory, i.e., its distance to the boundary of $\mathcal{S}$ at time $t = \tau, 2\tau, \ldots, k\tau$, and
2) check that this margin is always greater than the error $\Delta(t)$ at time $t = \tau, 2\tau, \ldots, k\tau$.

The complexity of these operations is very low.

C. Comparison with related work

We distinguish between works dealing with problem P1 and those dealing with P2.

- Problem P1: In many papers of the literature on SL methods with state constraints (see, e.g., [10]), the authors enforce the trajectory system to stay in $\mathcal{S}$ by introducing a (somehow artificial) "penalization" term in the cost function J, making the cost of crossing the boundary of $\mathcal{S}$ prohibitive (cf. [11]). In order to guarantee the result of convergence of $v^{\tau,\varepsilon}$ to v^{τ}, they also often make a restrictive assumption of "controllability". Note however that, in works like [1], [4], [5], no controllability assumption is made.
  In [23] (cf. [24]), the authors construct a sequence of abstractions which are more and more precise. The sequence of value function associated with each abstraction *converges* to the optimal value function associated the original problem. The abstract transition function computes an over-approximation of the set of trajectories starting at neighbouring points. This over-approximation is computed using a growth bound (bounding the distance of neighboring trajectories) based on the Jacobian matrix of f_a. More precisely, the growth bound is a function mapping any $\mathbf{r} \in \mathbb{R}^n_{\ge 0}$ to $e^{Mt}\mathbf{r}$, where M is a $n \times n$-matrix whose (i,j)-entry is $D_j f^i_a(z)$, if $i = j$ and $|D_j f^i_a(z)|$ otherwise, and $f^i_a(z)$ denotes the i-th component of vector $f_a(z)$. By comparison, our work here can be seen as a particular case of [23] where one uses, for each of the n components, a uniform growth bound, mapping $r \in \mathbb{R}_{\ge 0}$ to $e^{\lambda_a t} r$. The counterpart of the convergence result of [23] for the value function, would state in our context that the synthesized control converge towards the optimal control as ε tends to 0. However, this does not seem true (unless adding very restrictive assumptions), which leads us to focus on problem P2 instead of P1.
- Problem P2: In the work of [25], [26], the authors pursue an objective similar to ours: providing a (finite time-horizon) optimal control procedure with a formal guarantee of constraint satisfaction (safety). However they do not use SL-schemes, but perform a reachability analysis based on over-approximative state set representations (*zonotopes*, cf. [14], [2]).
  In [8], the authors also provide a formal guarantee of safety property. Contrarily to [25], [26], they do use SL-schemes. They also focus to (periodically) sampled systems as we do. However, they still perform a form of reachability analysis similar to [25], [26], using convex polytopes as state set representations. Their growth bound are not based on OSL constants as here, but rather on overapproximations of Lagrange remainders in Taylor series.

III. Sufficient Conditions for Reachability with Safety

Given a starting point $z_0 \in \mathcal{S}$ and a mode $a \in A$, we denote by $\tilde{X}^a_{\tau,y}$ the Euler-based image of z_0 at time $t = \tau$ via a. We have:

$$\tilde{X}^a_{\tau,z_0} := z_0 + \tau\ f_a(z_0).$$

The *set of admissible modes for* $x \in \mathcal{X}$ is defined by:

$$A_\tau(x) := \{a \in A \mid \tilde{X}^a_{\tau,x} \in \mathcal{S}\}.$$

The function $next^a : \mathcal{X} \to \mathcal{X} \cup \{\perp\}$ is defined by:

- if $a \in A_\tau(x)$, then: $next^a(x) = x'$, where x' is the ε-representative $\tilde{X}^a_{\tau,x}$,
- otherwise (i.e., $\tilde{X}^a_{\tau,x} \notin S$): $next^a(x) = \perp$.

For a pattern $\pi \in A^k$, the function $next^\pi : \mathcal{X} \to \mathcal{X} \cup \{\perp\}$ is defined as follows:

- if $\pi = a$ for some $a \in A$, then $next^\pi(x) = next^a(x)$,
- if π is of the form $a \cdot \pi'$;
  - if $next^a(x) \ne \perp$, then $next^\pi(x) = next^{\pi'}(next^a(x))$,
  - otherwise, $next^\pi(x) = \perp$.

It is easy to show, using the definition of $next$:

Proposition 1: Let $x \in \mathcal{X}$, and $\pi_k \in A^k$ a pattern of the form $a_k\ a_{k-1}\cdots\ a_1$. Let us write $\pi_i := a_k \cdots a_i$ for $1 \le i \le k$, and $x_{k+1} := x$.

If $next^{\pi_k}(x) \in \mathcal{X}$, then there exists a sequence of points of the form $x_{k+1}x_k \cdots x_1 \in \mathcal{X}^{n+1}$ with, for all $1 \le i \le k$:

- $\tilde{X}^{a_i}_{\tau,x_{i+1}} \in \mathcal{S}$,
- $x_i = next^{a_i}(x_{i+1}) = next^{\pi_i}(x)$, and
- $\|x_i - \tilde{X}^{a_i}_{\tau,x_{i+1}}\| \leq \varepsilon$.

Definition 1: For all point $x \in \mathcal{X}$, the *spatially discrete value function* $\mathbf{v}^{\tau,\varepsilon}_k : \mathcal{X} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ is defined by:

- for $k = 0$, $\mathbf{v}^{\tau,\varepsilon}_k(x) = \|x\|$,
- for $k \geq 1$,
  - if $A_\tau(x) = \emptyset$: $\mathbf{v}^{\tau,\varepsilon}_k(x) = \infty$,
  - if $A_\tau(x) \neq \emptyset$: $\mathbf{v}^{\tau,\varepsilon}_k(x) = \min_{a \in A_\tau(x)}\{\mathbf{v}^{\tau,\varepsilon}_{k-1}(next^a(x))\}$.

If $\mathbf{v}^{\tau,\varepsilon}_k(x) \neq \infty$, one defines the *approximate optimal pattern of length* k associated to x, denoted by $\pi^{\tau,\varepsilon}_k(x) \in A^k$, recursively by:

- if $k = 0$, $\pi^{\tau,\varepsilon}_k(x) = \text{nil}$,
- if $k \geq 1$, $\pi^{\tau,\varepsilon}_k(x) = \mathbf{a}_k(x) \cdot \pi'$ where

$$\mathbf{a}_k(x) = arg \min_{a \in A_\tau(x)} \{\mathbf{v}^{\tau,\varepsilon}_{k-1}(next^a(x))\}$$

  and $\pi' = \pi^{\tau,\varepsilon}_{k-1}(x')$ with $x' = next^{\mathbf{a}_k(x)}(x)$.

Using the value function $\mathbf{v}^{\tau,\varepsilon}_k$ it is thus easy to construct an SL procedure $PROC^{\tau,\varepsilon}_k$ which takes a point $x \in \mathcal{X}$ as input, and returns, in case of success (i.e., when $\mathbf{v}^{\tau,\varepsilon}_k(x) \geq 0$), a pattern $\pi^{\tau,\varepsilon}_k \in A^k$ with $next^{\pi^{\tau,\varepsilon}_k}(x) \in \mathcal{X}$. We now define, for such a pattern $\pi^{\tau,\varepsilon}_k$ output by $PROC^{\tau,\varepsilon}_k(x)$, a value $\Delta(\pi^{\tau,\varepsilon}_k)$ which gives us an *upperbound* to $\|X^{\pi^{\tau,\varepsilon}_k}_{k\tau,z_0} - next^{\pi^{\tau,\varepsilon}_k}(x)\|$, for any $z_0 \in B(x,\varepsilon)$ (i.e., any z_0 such that : $\|z_0 - x\| \leq \varepsilon$).

Definition 2: Let μ be a given positive constant. Let us define, for all $a \in A$ and $t \in [0,\tau]$, $\delta^a_{t,\mu}$ as follows:

- if $\lambda_a < 0$:

$$\delta^a_{t,\mu} = \left(\mu^2 e^{\lambda_a t} + \frac{C_a^2}{\lambda_a^2}\left(t^2 + \frac{2t}{\lambda_a} + \frac{2}{\lambda_a^2}\left(1 - e^{\lambda_a t}\right)\right)\right)^{\frac{1}{2}}$$

- if $\lambda_a = 0$:

$$\delta^a_{t,\mu} = \left(\mu^2 e^t + C_a^2(-t^2 - 2t + 2(e^t - 1))\right)^{\frac{1}{2}}$$

- if $\lambda_a > 0$:

$$\delta^a_{t,\mu} = \Big(\mu^2 e^{3\lambda_a t} + \frac{C_a^2}{3\lambda_a^2}\left(-t^2 - \frac{2t}{3\lambda_a} + \frac{2}{9\lambda_a^2}\left(e^{3\lambda_a t} - 1\right)\right)\Big)^{\frac{1}{2}}$$

where C_a and λ_a are constants defined in Section II-A.

Proposition 2: [6] Given $x \in \mathbb{R}^n$, we have, for all $a \in A$ and all $z_0 \in B(x,\varepsilon)$ (i.e., z_0 such that $\|z_0 - x\| \leq \varepsilon$):

$$\|X^a_{\tau,z_0} - \tilde{X}^a_{\tau,x}\| \leq \delta^a_{\tau,\varepsilon}.$$

Definition 3: Let us define $\Delta(a_k \cdots a_1)$ recursively by:

- $\Delta(a_i) = \delta^{a_i}_{\tau,\varepsilon}$ for $i = 1$, and
- $\Delta(a_i \cdots a_1) = \delta^{a_i}_{\tau,\mu}$ with $\mu = \varepsilon + \Delta(a_{i-1} \cdots a_1)$, for $i \geq 2$.

In the rest of the paper, we suppose that $k \in \mathbb{N}$ and $\tau, \varepsilon \in \mathbb{R}_{>0}$ are given and fixed. So, for the sake of notation simplicity, we will abbreviate $\mathbf{v}^{\tau,\varepsilon}_k$ as $\mathbf{v}_k$. We abbreviate similarly $\pi^{\tau,\varepsilon}_k$ and $PROC^{\tau,\varepsilon}_k$ as π_k and $PROC_k$ respectively. We will suppose also that we are given a compact set $\mathcal{S} \subset \mathbb{R}^n$ as well as a "target" set $R \subset \mathcal{S}$.[1] We have:

Lemma 1: Let $x \in \mathcal{X}$ and $\pi_k \equiv a_k \cdots a_1 \in A^k$ the pattern generated by $PROC_k(x)$ with $next^{\pi_k}(x) \in \mathcal{X}$. We have, for all $z_0 \in B(x,\varepsilon)$:

1) $\|X^{\pi_k}_{k\tau,z_0} - \tilde{X}^{a_1}_{\tau,x_2}\| \leq \Delta(\pi_k)$,
   with $x_2 := next^{a_k \cdots a_2}(x)$ for $k \geq 2$, and $x_2 := x$ for $k = 1$;
2) $\|X^{\pi_k}_{k\tau,z_0} - next^{\pi_k}(x)\| \leq \Delta(\pi_k) + \varepsilon$.

Proof: Let us prove items 1-2 by induction on k.

Let us first prove item 1 for the base case $k = 1$. We have $\pi_k = \pi_1 = a_1$ and $x_2 = x$. We have to prove, when $\|x - z_0\| \leq \varepsilon$: $\|X^{a_1}_{\tau,z_0} - \tilde{X}^{a_1}_{\tau,x}\| \leq \Delta(a_1) = \delta^{a_1}_{\tau,\varepsilon}$. This inequation holds by Proposition 2, and the proof of item 1 is done. The proof of item 2 of the base case follows from item 1 and Proposition 1, using triangular inequality.

Let us now consider the induction step. We have to prove the following induction conclusion:

1) $\|X^{a_{k+1} \cdots a_1}_{(k+1)\tau,z_0} - \tilde{X}^{a_1}_{\tau,x_2}\| \leq \Delta(a_{k+1} \cdots a_1)$,
   with $x_2 := next^{a_k \cdots a_2}(x)$
2) $\|X^{a_{k+1} \cdots a_1}_{(k+1)\tau,z_0} - next^{a_{k+1} \cdots a_1}(x)\| \leq \Delta(a_{k+1} \cdots a_1) + \varepsilon$.

We have by induction hypothesis:

1) $\|X^{a_{k+1} \cdots a_2}_{k\tau,z_0} - \tilde{X}^{a_2}_{\tau,x_3}\| \leq \Delta(a_{k+1} \cdots a_2)$,
   with $x_3 := next^{a_{k+1} \cdots a_2}(x)$, and
2) $\|X^{a_{k+1} \cdots a_2}_{k\tau,z_0} - next^{a_{k+1} \cdots a_2}(x)\| \leq \mu$,
   with $\mu := \Delta(a_{k+1} \cdots a_2) + \varepsilon$.

Besides, by Definition 3: $\Delta(a_{k+1} \cdots a_1) = \delta^{a_1}_{\tau,\mu}$.
Applying Proposition 2, with $z_2 = X^{a_{k+1} \cdots a_2}_{k\tau,z_0}$ and $x_2 = next^{a_{k+1} \cdots a_2}(x)$, we have:

$$\|X^{a_1}_{\tau,z_2} - \tilde{X}^{a_1}_{\tau,x_2}\| \leq \delta^{a_1}_{\tau,\mu}$$

since $\|x_2 - z_2\| \leq \mu$ by item 2 of induction hypothesis. It follows

$$\|X^{a_{k+1} \cdots a_1}_{(k+1)\tau,z_0} - \tilde{X}^{a_1}_{\tau,x_2}\| \leq \delta^{a_1}_{\tau,\mu} = \Delta(a_{k+1} \cdots a_1).$$

This achieves the proof of the item 1 of the induction conclusion. The item 2 of the induction conclusion then follows from item 1 and Proposition 1, using triangular inequality. This completes the proof of the induction step. ∎

[1] We suppose implicitly that R contains the target point z_{ref}, so R can be seen as a neighborhood of z_{ref}.

Using item 2 of Lemma 1, it is easy to show:

Theorem 1: (sufficient conditions of safety and k-reachability) Let $x \in \mathcal{X}$, and $\text{ß}_k \equiv a_k \cdots a_1 \in A^k$ the pattern generated by $PROC_k(x)$ with $next^{\pi_k}(x) \in \mathcal{X}$. Suppose, for all $1 \leq i \leq k$:

- (H_1^i): $B(next^{\pi_i}(x), \Delta(\pi_i) + \varepsilon) \subseteq \mathcal{S}$, and
- (H_2^k): $B(next^{\pi_k}(x), \Delta(\pi_k) + \varepsilon) \subseteq R$,

where $\pi_i := a_k \cdots a_i$. Then we have, for all $z_0 \in B(x, \varepsilon)$[2]

- $X^{\pi_i}_{(k-i+1)\tau, z_0} \in S$ for all $1 \leq i \leq k$ (*discrete-time safety*), and
- $X^{\pi_k}_{k\tau, z_0} \in R$ (*k-reachability*).

Furthermore, assuming that, for all $a \in A$, $\delta^a_{t,\varepsilon}$ is a convex function for $t \in [0, \tau]$ (i.e., $\frac{d^2(\delta^a_t)}{dt^2} > 0$ for all $t \in [0, \tau]$ [3]), we have:

$X^{\pi_k}_{t, z_0} \in S$ for all $t \in [0, k\tau]$ (*dense-time safety*).

Suppose in particular that conditions (H_1^i)-(H_2^k) hold for a set of points $\mathcal{Y} \subseteq \mathcal{X}$ which ε-*covers* R, i.e., such that: $R \subseteq \bigcup_{x \in \mathcal{Y}} B(x, \varepsilon)$. In this case, the procedure $PROC_k$ gives us a guarantee of "(R, S)-stability" as defined in [13]. By Theorem 1, we know indeed that, for all $z_0 \in R$ of representative $x \in \mathcal{X}$, the pattern π_k generated by $PROC_k(x)$ applied to z_0 yields a trajectory that reaches at $t = k\tau$ a point z' of R (while always staying in $\mathcal{S}$ for $0 \leq t \leq k\tau$); the process can then be iterated to z', and so on repeatedly. This means that, via the set of patterns π_k associated to elements of $\mathcal{Y}$, one can control any trajectory starting at R in order to make it return to R periodically every $k\tau$ seconds, and stay in $\mathcal{S}$ for all $t \geq 0$ ("(R, S)-stability").[4]

The SL-based procedure $PROC_k$ can thus replace advantageously the brute-force enumeration strategy implemented in tool MINIMATOR [19]: the time complexity of MINIMATOR procedure is indeed $O(m^k \times N)$ where m is the number of modes, N the number of cells and k the time-horizon length, while the complexity of $PROC_k$ is $O(m \times k \times N)$.

A. Description of the implementation

The procedure is implemented in Octave. It is composed of 9 functions and a main script totalling 500 lines of code. For comparison, the tool MINIMATOR uses 28 functions for a total of 2000 lines of code.

[2]In particular, for any $z_0 \in S$ of ε-representative x.

[3]The sign of $\frac{d^2(\delta^a_t)}{dt^2}$ on $[0, \tau]$ depends on the value of the constants C_a and λ_a occurring in Definition 2; knowing these constant values, the sign is easy to determine (see [6]).

[4]R can be seen as a special case of *viability kernel* for $\mathcal{S}$ (see, e.g., [3]) since any trajectory starting from R can be controlled in order to stay inside $\mathcal{S}$ forever.

The computations are realised in a virtual machine running Ubuntu 18.06 LTS, having access to one core of a 2.3GHz Intel Core i5, associated to 3.5GB of RAM memory.

Note that the accuracy of the Euler approximation can be optionally increased by using a smaller time step. The time-step h used for Euler approximation is not necessarily equal to the control sampling period, but is in general a *submultiple* of τ ($\tau = p \times h$ where p is a natural number greater than 1).

Example 1: (2-tanks)
In this example, we illustrate the approach given above for (R, S)-stability on a two tank example. The two-tank system is a linear example taken from [17]. The system consists of two tanks and two valves. The first valve adds to the inflow of tank 1 and the second valve is a drain valve for tank 2. There is also a constant outflow from tank 2 caused by a pump. The system is linearized at a desired operating point. The objective is to keep the water level in both tanks within limits using a discrete open/close switching strategy for the valves. Let the water level of tanks 1 and 2 be given by x_1 and x_2 respectively. The behavior of x_1 is given by $\dot{x}_1 = -x_1 - 2$ when the tank 1 valve is closed, and $\dot{x}_1 = -x_1 + 3$ when it is open. Likewise, x_2 is driven by $\dot{x}_2 = x_1$ when the tank 2 valve is closed and $\dot{x}_2 = x_1 - x_2 - 5$ when it is open.

Let $S = [-2, 3] \times [-1, 2]$, $R = [-1.5, 2.5] \times [-0.5, 1.5]$, $N = 10 \times 10$ the number of cells, $\varepsilon = 0.33$, $\tau = 0.1$. The proof of (R, S)-stability is obtained for $k = 5$, it takes 7.34 seconds. By comparison, MINIMATOR takes 25.53 seconds to obtain a controller without any optimality result. Simulations of the (R, S)-stability controller are given in Figure 1.

IV. Extensions

We now explain how to extend the method to stochastic ODEs and differential games.

A. Stochastic switched systems

Let us consider a stochastic switched system defined by

$$\mathrm{d}X_t = f_a(X_t)\mathrm{d}t + g_a(X_t)\mathrm{d}W_t, \qquad X_0 = x_0, \qquad (7)$$

where W_t is a standard $m-dimensional$ Brownian motion, and suppose that for all $a \in A$:

(H1) $f_a : \mathbb{R}^n \to \mathbb{R}^n$ is a continuously differentiable function whose derivative grows at most polynomially,

(H2) $g_a = (g_{a_{i,j}})_{i \in \{1,\ldots,n\}, j \in \{1,\ldots,m\}} : \mathbb{R}^n \to \mathbb{R}^{n \times m}$ is a globally Lipschitz continuous function,

(H3) f_a is globally one-sided Lipschitz.

Under the above-mentioned hypotheses, we can establish bounds $\delta^a_{t,\varepsilon}$ similar to Definition 2 for stochastic switched systems using the *tamed Euler scheme* [16]. The detail of this bound is given in Appendix for a single mode stochastic switched system (*i.e.* a stochastic differential equation). We refer the reader to [20] for the details of the error bounding for stochastic switched systems. The result is stated as

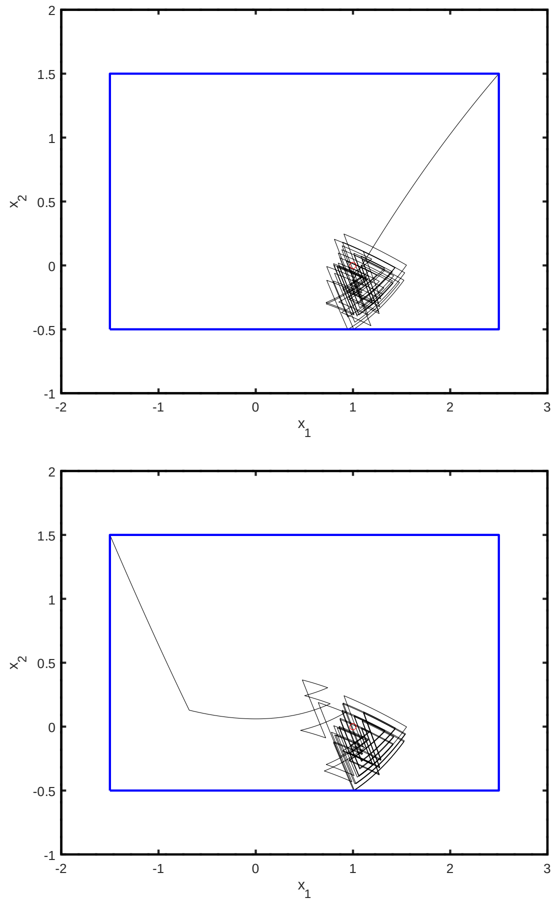

Fig. 1. Simulations of the (R, S)-stability controller on the two tank example. The safety set is $S = [-2, 3] \times [-1, 2]$, the recurrence set $R = [-1.5, 2.5] \times [-0.5, 1.5]$, the blue box is the set R, the red circle is the objective here chosen as $(1.0, 0.0)$. The trajectory of the system is in black for two initial conditions: $(2.5, 2.5)$ (top) and $(-1.5, 1.5)$ (bottom).

follows for a single switching step integration:

Proposition 3 ([20]): Consider two points x_0 and z in $\mathbb{R}^n$,and a positive real number ε. Suppose that $x_0 \in B(z, \varepsilon)$. Let us denote by $\tilde{X}_{t,z}$ the tamed Euler approximation of X_t starting from initial point z in (7). Then $\mathbb{E}X_{t,x_0} \in B(\tilde{X}_{t,z}, \delta^a_{t,\varepsilon})$ for all $t \in [0, \tau]$, where $\mathbb{E}$ is the symbol of expected value.

Example 2: (Stochastic system) Consider the system (see ([28], [27])):

$$dx_1 = (-0.25x_1 + ux_2 + (-1)^u 0.25)dt + 0.01x_1 dW_t^1$$
$$dx_2 = ((u-3)x_1 - 0.25x_2 + (-1)^u(3-u))dt + 0.01x_2 dW_t^2$$

where $u = 1, 2$.

We can apply the above procedure $PROC_k^{\tau,\varepsilon}$ in order to minimize the average distance of the state to the origin after a given number of steps. We consider a switching period $\tau = 0.5$ subdivided in time steps of size $\Delta_t = 10^{-4}$. Consider the interest set $R = B((0, 0), \rho)$ with $\rho = 7$, discretized with an accuracy $\varepsilon = 0.57$. We compute (sub)optimal patterns for the entire set, using different lengths of patterns, and simulate the induced controller for 200 initial conditions randomly selected in R. Simulations are given in Figure 2. The procedure took 11.8 seconds of computation for patterns of length 1, 47.4 seconds of computation for patterns of length 3.

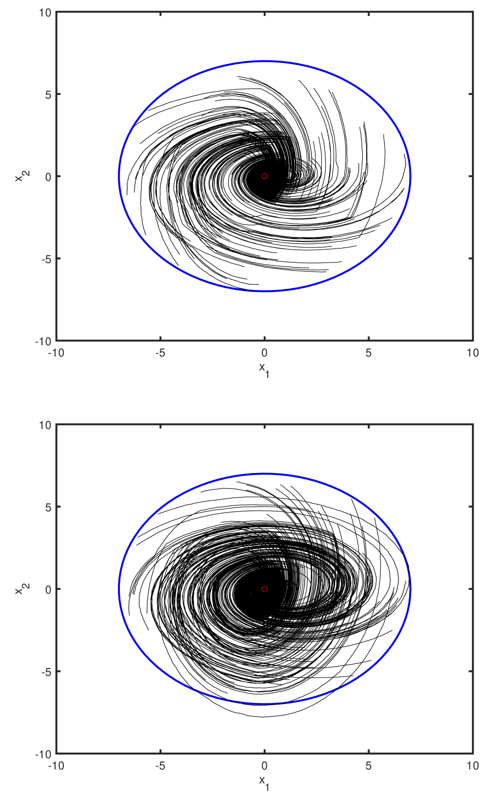

Fig. 2. Simulations of Example 2 with the controller induced by $PROC_k$, for patterns of length 1 (top), length 3 (bottom). The blue circle is the set $R = B((0, 0), 7)$, the red marker is the target state (the origin), the black lines are the controlled trajectories.

B. Sampled Pursuit-Evasion Games with Safety

Let us explain here how one can extend our SL-based method to Pursuit-Evasion games, closely following the work of [7]. The ODEs are defined by:

$$(\dot{z}_1(t), \dot{z}_2(t)) = (f_a^1(z_1(t)), f_b^2(z_2(t))), \qquad t > 0$$
$$(z_1(0), z_2(0)) = (z_1^0, z_2^0)$$

where $(z_1(t), z_2(t)) \in \mathbb{R}^n \times \mathbb{R}^n$, $(z_1^0, z_2^0) \in \mathbb{R}^n \times \mathbb{R}^n$, $a \in A$, $b \in B$, and f_a^1 and f_b^2 are functions of $\mathbb{R}^n \to \mathbb{R}^n$. Given a safety set $\mathcal{S} = S_1 \times S_2 \subset \mathbb{R}^n \times \mathbb{R}^n$, the (dense-time) safety constraint is: $z_1(t) \in S_1$, $z_2(t) \in S_2$. The target set is defined by:

$$R = \{(z_1, z_2) \in \mathbb{R}^n \times \mathbb{R}^n : \ \|z_1 - z_2\| \leq \gamma\}, \ \ \gamma \geq 0$$

Example 3: (The Tag-Chase game with constraints) [7]

Two players 1 (pursuer) and 2 (evader) which run one after the other in the same 2-dimensional domain (courtyard), so that the game is set in $\mathcal{S} = S_1^2 \subset \mathbb{R}^4$. Players 1 and 2 can run in every direction with velocity V_1 and V_2 respectively. The control sets are of the form

$$A = \{\alpha_1, \dots, \alpha_{m_1}\}, \quad B = \{\beta_1, \dots, \beta_{m_2}\}.$$

We have the dynamics for $z_1 = (i_1, j_1)$ and $z_2 = (i_2, j_2)$:

$$\begin{array}{lll} 1: & \dot{i_1} = V_1 \ sin\alpha \ \ ; & \dot{j_1} = V_1 \ cos\alpha \\ 2: & \dot{i_2} = V_2 \ sin\beta \ \ ; & \dot{j_2} = V_2 \ cos\beta \end{array}$$

where $\alpha \in A$ is the direction for 1, and $\beta \in B$ is the direction for 2 (α and β are the angles between the j-axis and the velocities for 1 and 2). For $z_1 \equiv (i_1, j_1)$ and $z_2 \equiv (i_2, j_2)$, the capture occurs when $z \equiv (z_1, z_2) \in R \equiv R_1 \times R_2$ with

$$R = \{((i_1, j_1), (i_2, j_2)) \in \mathcal{S} : \sqrt{(i_1 - i_2)^2 + (j_1 - j_2)^2} \le \gamma\}.$$

We build a partition of $\mathcal{S} = S_1 \times S_2$ and construct a grid $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_2$ by performing separately the operations described in Section III on $\mathcal{S}_1$ and $\mathcal{S}_2$.

Definition 4: For $x = (x_1, x_2) \in \mathcal{X}$, the *sets of admissible controls* $A_\tau(x_1)$ and $B_\tau(x_2)$ w.r.t. $\mathcal{S}_1$ and $\mathcal{S}_2$ respectively, are defined by:

$$A_\tau(x_1) = \{a \in A : \ x_1 + \tau f_a^1(x_1) \in S_1\},$$

$$B_\tau(x_2) = \{b \in B : \ x_2 + \tau f_b^2(x_2) \in S_2\}.$$

Let denote by $next^{a,b} : \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{X}_1 \times \mathcal{X}_2$, the function defined, for $x = (x_1, x_2)$ by:

$$next^{a,b}(x) := (next^a(x_1), next^b(x_2)),$$

where $next^a : \mathcal{X}_1 \to \mathcal{X}_1$ and $next^b : \mathcal{X}_2 \to \mathcal{X}_2$ are defined as in Section III.

Definition 5: The *value function* $\mathbf{v}_k : \mathcal{X} \to \mathbb{R}_{\ge 0} \cup \{\infty\}$ is defined, for all $x \equiv (x_1, x_2) \in \mathcal{X}$ with $x_1 \equiv (i_1, j_1)$ and $x_2 \equiv (i_2, j_2)$, by:

- For $k = 0$, $\mathbf{v}_k(x) = \sqrt{(i_1 - i_2)^2 + (j_1 - j_2)^2}$;
- For $k \ge 1$,
  - if $A_\tau(x_1) = \emptyset \ \vee \ B_\tau(x_2) = \emptyset$, $\mathbf{v}_k(x) = \infty$;
  - if $A_\tau(x_1) \neq \emptyset \ \wedge \ B_\tau(x_2) \neq \emptyset$,

$$\mathbf{v}_k(x) = \max_{b \in B_\tau(x_2)} \min_{a \in A_\tau(x_1)} \{\mathbf{v}_{k-1}(next^{a,b}(x))\}.$$

Similarly to what has been done in Section III, one can construct, for $x = (x_1, x_2) \in \mathcal{X}$ with $\mathbf{v}_k(x) \ge 0$, a procedure $PROC_k$ which returns a pattern $(\pi_k^1, \pi_k^2) \in A^k \times B^k$ with $next^{\pi_k^1}(x_1) \in \mathcal{X}_1$ and $next^{\pi_k^2}(x_2) \in \mathcal{X}_2$.[5] The counterpart of Theorem 1 is:

Theorem 2: (sufficient conditions of safety and k-capture) Consider a point $x = (x_1, x_2) \in \mathcal{X}$, and let $(\pi_k^1, \pi_k^2) \equiv (a_k \cdots a_1, b_k \cdots b_1)$ be the pattern generated by $PROC_k(x)$ with $next^{\pi_k^1}(x_1) \in \mathcal{X}_1$ and $next^{\pi_k^2}(x_2) \in \mathcal{X}_2$. Suppose that, for all $1 \le i \le k$:

1) $B(next^{a_k \cdots a_i}(x_1), \Delta(a_k \cdots a_i) + \varepsilon) \subseteq \mathcal{S}_1$ and $B(next^{b_k \cdots b_i}(x_2), \Delta(b_k \cdots b_i) + \varepsilon) \subseteq \mathcal{S}_2$, and
2) $B(next^{a_k \cdots a_1}(x_1), \Delta(a_k \cdots a_1) + \varepsilon) \subseteq R_1$ and $B(next^{b_k \cdots b_1}(x_2), \Delta(b_k \cdots b_1) + \varepsilon) \subseteq R_2$.

Then we have for all $z = (z_1, z_2) \in B(x_1, \varepsilon) \times B(x_2, \varepsilon)$, and all $i \in \{1, \dots, k\}$:

- $X^{a_k \cdots a_i}_{(k-i+1)\tau, z_1} \in S_1$ and $X^{b_k \cdots b_i}_{(k-i+1)\tau, z_2} \in S_2$ (safety), and
- $(X^{a_k \cdots a_1}_{k\tau, z_1}, X^{b_k \cdots b_1}_{k\tau, z_2}) \in R.$ (k-capture).

[5]Note that the 1st element of the sequence $(\pi_k^1, \pi_k^2) \in A^k \times B^k$ is of the form $(\mathbf{a}_k, \mathbf{b}_k) = arg \max_{b \in B_\tau(x_2)} \min_{a \in A_\tau(x_1)} \{\mathbf{v}_{k-1}(next^{a,b}(x))\}$.

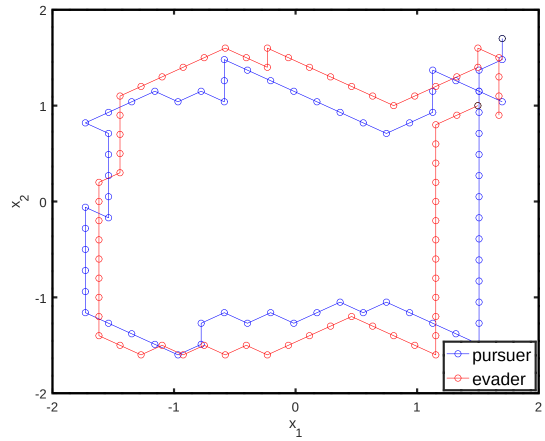

Fig. 3. Simulations of the tag-chase game. The initial states are $z_1 = (1.7, 1.7)$, $z_2 = (1.5, 1.0)$. The capture states are $z_1 = (1.7, 1.04)$, $z_2 = (1.67, 0.9)$.

Example 4: (Tag-Chase game) Let us consider Example 3 with $V_1 = 2$, $V_2 = 1$, $S = [-2, 2]^4$, $m_1 = m_2 = |A| = |B| = 6$, $A = B = \{\pm\pi/3, \pm\pi/2, \pm 2\pi/3\}$. Let the target R be defined by: $R = \{(z_1, z_2) \in \mathbb{R}^4 : \|z_1 - z_2\| \le 0.7\}$.

Let $N = 10$ the number of nodes in each dimension, $\varepsilon = 0.31$, $\tau = 0.2$. One can check that conditions 1 and 2 of Theorem 2 are satisfied for $k = 1$. Applying the corresponding strategy to $z = (z_1, z_2)$ with $z_1 = (1.7, 1.7)$, $z_2 = (1.5, 1.0)$, it can be shown that the controlled trajectory, after 66 steps, reaches the state $z_1 = (1.7, 1.04)$, $z_2 = (1.67, 0.9)$ which belongs to the target R. See the controller simulation Figure 3 where the player 1 (pursuer) is in blue, and the player 2 (evader) in red. For this initial state, one can observe that, at step 68, a limit cycle of length 16 is reached (see Figure 4). Note that, for other initial states, the length of the limit cycle may be different, and is often 2. The experiment takes 534 seconds of CPU time.

V. Final Remarks

We have presented a new SL-based method for synthesizing a provably safe finite-time horizon control. We have illustrated the interest of the method on a classical example (2-tanks) and shown how to extend it to stochastic ODEs and

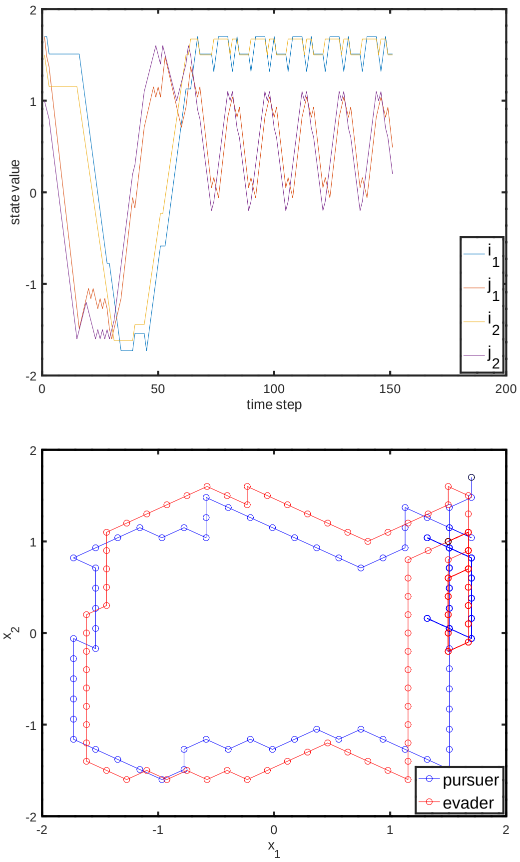

Fig. 4. Simulations of the tag-chase game. The initial states are $z_1 = (1.7, 1.7)$, $z_2 = (1.5, 1.0)$. At step 68, a limit cycle of length 16 is reached.

differential games. The potential application of such methods to Model Predictive Control has been pointed in [25].

A defect of our method is that, in order to satisfy the sufficient conditions of Theorem 1, one may have to decrease the cell size ε too much, thus making the number of cells explode, as often in SL methods. In this case, methods using symbolic reachability analysis, such as in [8], [25], [26], may be more efficient. A comparative experimental work between the two kinds of method is planned for future work.

References

[1] Albert Altarovici, Olivier Bokanowski, and Hasnaa Zidani. A general hamilton-jacobi framework for non-linear state-constrained control problems. *ESAIM: Control, Optimisation and Calculus of Variations*, 19(2):337–357, 2013.

[2] Matthias Althoff and Bruce H Krogh. Zonotope bundles for the efficient computation of reachable sets. In *2011 50th IEEE Conference on Decision and Control and European Control Conference*, pages 6814–6821. IEEE, 2011.

[3] Jean-Pierre Aubin and Hélène Frankowska. The viability kernel algorithm for computing value functions of infinite horizon optimal control problems. *Journal of mathematical analysis and applications*, 201(2):555–576, 1996.

[4] Olivier Bokanowski, Nicolas Forcadel, and Hasnaa Zidani. Reachability and minimal times for state constrained nonlinear problems without any controllability assumption. *SIAM Journal on Control and Optimization*, 48(7):4292–4316, 2010.

[5] Pierre Cardaliaguet, Marc Quincampoix, and Patrick Saint-Pierre. Pursuit differential games with state constraints. *SIAM Journal on Control and Optimization*, 39(5):1615–1632, 2000.

[6] Adrien Le Coënt, Florian De Vuyst, Ludovic Chamoin, and Laurent Fribourg. Control synthesis of nonlinear sampled switched systems using euler's method. *In SNR'17, EPTCS 247, pages 18-33, Open Publishing Association.*, 2017.

[7] Emiliano Cristiani and Maurizio Falcone. Fully-discrete schemes for the value function of pursuit-evasion games with state constraints. In *Advances in dynamic games and their applications*, pages 1–30. Springer, 2009.

[8] J Estrela da Silva, João Tasso Sousa, and Fernando Lobo Pereira. Synthesis of safe controllers for nonlinear systems using dynamic programming techniques. 2017.

[9] Tzanko Donchev and Elza Farkhi. Stability and euler approximation of one-sided lipschitz differential inclusions. *SIAM journal on control and optimization*, 36(2):780–796, 1998.

[10] Maurizio Falcone. Numerical solution of dynamic programming equations. *Optimal Control and Viscosity Solutions of Hamilton-Jacobi-Bellman equations. Birkhäuser*, 1997.

[11] Maurizio Falcone and Roberto Ferretti. Semi-lagrangian schemes for hamilton–jacobi equations, discrete representation formulae and godunov methods. *Journal of computational physics*, 175(2):559–575, 2002.

[12] Roberto Ferretti and Hasnaa Zidani. Monotone numerical schemes and feedback construction for hybrid control systems. *Journal of Optimization Theory and Applications*, 165(2):507–531, 2015.

[13] Laurent Fribourg, Ulrich Kühne, and Romain Soulat. Finite controlled invariants for sampled switched systems. *Formal Methods in System Design*, 45(3):303–329, 2014.

[14] Antoine Girard. Reachability of uncertain linear systems using zonotopes. In *International Workshop on Hybrid Systems: Computation and Control*, pages 291–305. Springer, 2005.

[15] Antoine Girard, Giordano Pola, and Paulo Tabuada. Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Transactions on Automatic Control*, 55(1):116–126, 2010.

[16] Desmond J. Higham, Xuerong Mao, and Andrew M. Stuart. Strong convergence of Euler-type methods for nonlinear stochastic differential equations. *SIAM Journal on Numerical Analysis*, 40(3):1041–1063, 2002.

[17] Ian A Hiskens. Stability of limit cycles in hybrid systems. In *Proceedings of the 34th Annual Hawaii International Conference on System Sciences*, pages 6–pp. IEEE, 2001.

[18] Martin Hutzenthaler, Arnulf Jentzen, and Peter E. Kloeden. Strong convergence of an explicit numerical method for SDEs with nonglobally lipschitz continuous coefficients. *Annals of Applied Probability*, 22(4):1611–1641, 2012.

[19] Ulrich Kühne and Romain Soulat. Minimator 1.0, `https://bitbucket.org/ukuehne/minimator/overview`, 2015.

[20] Adrien Le Coënt, Laurent Fribourg, and Jonathan Vacher. Control synthesis for stochastic switched systems using the tamed euler method. *IFAC-PapersOnLine*, 51(16):259–264, 2018.

[21] Frank Lempio. Set-valued interpolation, differential inclusions, and sensitivity in optimization. In *Recent developments in well-posed variational problems*, pages 137–169. Springer, 1995.

[22] B.K. Oksendal. *Stochastic Differential Equations: An Introduction with Applications*. Springer, 2002.

[23] Gunther Reissig and Matthias Rungger. Symbolic optimal control. *IEEE Transactions on Automatic Control*, 2018.

[24] Matthias Rungger and Gunther Reissig. Arbitrarily precise abstractions for optimal controller synthesis. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pages 1761–1768. IEEE, 2017.

[25] Bastian Schürmann and Matthias Althoff. Guaranteeing constraints of disturbed nonlinear systems using set-based optimal control in generator space. *IFAC-PapersOnLine*, 50(1):11515–11522, 2017.

[26] Bastian Schürmann and Matthias Althoff. Optimal control of sets of solutions to formally guarantee constraints of disturbed linear systems. In *2017 American Control Conference (ACC)*, pages 2522–2529. IEEE, 2017.

[27] Majid Zamani, Alessandro Abate, and Antoine Girard. Symbolic models for stochastic switched systems: A discretization and a discretization-free approach. *Automatica*, 55:183–196, 2015.

[28] Majid Zamani, Peyman Mohajerin Esfahani, Rupak Majumdar, Alessandro Abate, and John Lygeros. Symbolic control of stochastic systems via approximately bisimilar finite abstractions. *IEEE Trans. Automat. Contr.*, 59(12):3135–3150, 2014.

VI. Appendix: error bounding for the tamed Euler scheme

A. Assumptions

The symbol $\|\cdot\|$ denotes the Euclidean norm on $\mathbb{R}^n$.The symbol $\langle\cdot,\cdot\rangle$ denotes the scalar product of two vectors of $\mathbb{R}^n$. Given a point $x \in \mathbb{R}^n$ and a positive real $r > 0$, the ball $B(x,r)$ of centre x and radius r is the set $\{y \in \mathbb{R}^n \mid \|x-y\| \leq r\}$.

Let $\tau \in (0,\infty)$ be a fixed real number, let $(\Omega,\mathcal{F},\mathbb{P})$ be a probability space with normal filtration $(\mathcal{F}_t)_{t\in[0,\tau]}$, let $n,m \in \mathbb{N} := \{1,2,\dots\}$ let $W = (W^{(1)},\dots,W^{(m)}) : [0,R]\times\Omega \to \mathbb{R}^m$ be an m-dimensional standard $(W_t)_{t\in[0,\tau]}$-Brownian motion and let $x_0 : \Omega \to \mathbb{R}^n$ be an $\mathcal{F}_0/\mathcal{B}(\mathbb{R}^n)$-measurable mapping with $\mathbb{E}[\|x_0\|^p] < \infty$ for all $p \in [1,\infty)$. Moreover, let $f : \mathbb{R}^n \to \mathbb{R}^n$ be a continuously differentiable function whose derivative grows at most polynomially. Formally, let us suppose the existence of constants $D \in \mathbb{R}_{\geq 0}$ and $q \in \mathbb{N}$ such that, for all $x,y \in \mathbb{R}^n$

$$\|f(x)-f(y)\|^2 \leq D\|x-y\|^2(1+\|x\|^q+\|y\|^q) \tag{H1}$$

Let $g = (g_{i,j})_{i\in\{1,\dots,d\},j\in\{1,\dots,m\}} : \mathbb{R}^n \to \mathbb{R}^{d\times m}$ be a globally Lipschitz continuous function: there exists $L_g \in \mathbb{R}_{\geq 0}$ such that, for all $x,y \in \mathbb{R}^n$

$$\|g(x)-g(y)\| \leq L_g\|x-y\| \tag{H2}$$

Finally, let us suppose that f is globally one-sided Lipschitz with constant $\lambda \in \mathbb{R}$:

$$\exists\lambda \in \mathbb{R}\ \forall x,y \in \mathbb{R}^n :\ \langle f(y)-f(x), y-x\rangle \leq \lambda\,\|y-x\|^2 \tag{H3}$$

Then consider the Stochastic Differential Equations (SDE):

$$\mathrm{d}X_t = f(X_t)\mathrm{d}t + g(X_t)\mathrm{d}W_t, \qquad X_0 = x_0 \tag{8}$$

for $t \in [0,\tau]$. The drift coefficient f is the infinitesimal mean of the process X and the diffusion coefficient g is the infinitesimal standard deviation of the process X. Under the above assumptions, the SDE (8) is known to have a unique strong solution. More formally, there exists an adapted stochastic process $X : [0,\tau]\times\Omega \to \mathbb{R}^n$ with continuous sample paths fulfilling

$$X_{t,x_0} = x_0 + \int_0^t f(X_s)\mathrm{d}s + \int_0^t g(X_s)\mathrm{d}W_s$$

for all $t \in [0,\tau]$ $\mathbb{P}$-a.s. (see, e.g., [22]).

We denote by X_{t,x_0} the solution of Equation (8) at time t from initial condition $X_{0,x_0} = x_0$ $\mathbb{P}$-a.s., in which x_0 is a random variable that is measurable in $\mathcal{F}_0$.

Remark 1: Constants λ, L_g and D can be computed using (constrained) optimization algorithms (see [6]).

B. Tamed Euler scheme

The standard time-discrete *tamed Euler scheme* is defined as a follows. Let $\underline{X}^N_{n,z} : \Omega \to \mathbb{R}^d$,

$$\underline{X}^N_{n+1,z} = \underline{X}^N_{n,z} + \frac{\frac{\tau}{N}\cdot f(\underline{X}^N_{n,z})}{1+\frac{\tau}{N}\cdot\|f(\underline{X}^N_{n,z})\|} + g(\underline{X}^N_{n,z})(W_{\frac{(n+1)\tau}{N}} - W_{\frac{n\tau}{N}}) \tag{9}$$

for all $n \in \{0,1,\dots,N-1\}$ and all $N \in \mathbb{N}$. In this method the drift term $\frac{\tau}{n}\cdot f(\underline{X}^N_{n,z})$ is "tamed" by the factor $1/(1+\frac{\tau}{N}\cdot\|f(\underline{X}^N_{n,z})\|)$ for $n \in \{0,1,\dots,N-1\}$ and $N \in \mathbb{N}$ in (9).

A time continuous interpolation of the tamed Euler scheme (introduced in [18]) is written as follows. Let $\tilde{X}^N_z : [0,\tau]\times\Omega \to \mathbb{R}^n$, $N \in \mathbb{N}$, be a sequence of stochastic processes given by

$$\tilde{X}^N_{t,z} = \tilde{X}^N_{n,z} + \frac{(t-n\tau/N)\cdot f(\tilde{X}^N_{n,z})}{1+\tau/N\cdot\|f(\tilde{X}^N_{n,z})\|} + g(\tilde{X}^N_{n,z})(W_t - W_{\frac{n\tau}{N}}) \tag{10}$$

for all $t \in [\frac{n\tau}{N},\frac{(n+1)\tau}{N}]$, $n \in \{0,1\dots,N-1\}$ and all $N \in \mathbb{N}$. Note that $\tilde{X}^N_{t,z} : [0,\tau]\times\Omega \to \mathbb{R}^n$ is an adapted stochastic process with continuous sample paths for every $N \in \mathbb{N}$.

Lemma 2: Let us suppose (H1) (H2) and (H3). Let the setting in this section be fulfilled, and $z : \Omega \to \mathbb{R}^n$ be an $\mathcal{F}_0/\mathcal{B}(\mathbb{R}^n)$-measurable mapping with $\mathbb{E}[\|z\|^p] < \infty$ for all $p \in [1,\infty)$. Then, for any even integer $r \geq 2$, there exist two constants $E_{r,z}$ and $F_{r,z}$ such that

$$\sup_{0\leq t\leq\tau}\mathbb{E}\|\underline{X}_{t,z} - \tilde{X}_{t,z}\|^r \leq (\Delta_t)^{\frac{r}{2}}(E_{r,z}(\Delta_t)^{\frac{r}{2}} + F_{r,z}d).$$

with $\Delta_t = \tau/N$ and:

$$E_{r,z} = 2^r(\|f(0)\|^r + D2^{\frac{r+1}{2}} (1+\mathbb{E}\sup_{0\leq t\leq\tau}\|\underline{X}_{t,z}\|^{qr})^{\frac{1}{2}}(\mathbb{E}\sup_{0\leq t\leq\tau}\|\underline{X}_{t,z}\|^{2r})^{\frac{1}{2}}),$$

$$F_{r,z} = 2^r(\|g(0)\|^{2r} + L_g^r\mathbb{E}\sup_{0\leq t\leq\tau}\|\underline{X}_{t,z}\|^{\frac{r}{2}}).$$

Remark 2: Constants $E_{r,z}$ and $F_{r,z}$ are computed using the constants λ and L_g (see Remark 1), and the expected values of $\underline{X}_{t,z}$ at each time $t = 0,\Delta t, 2\Delta t,\dots,N\Delta t$. These expected values are computed using a Monte Carlo method (by averaging here the value of 10^4 samplings).

C. Mean square error bounding

The following Theorem holds for SDE (8). This corresponds to a stochastic version of Theorem 1 of [6], showing that a similar result holds on average, using the tamed Euler method of [18]. It is an adaptation of Theorem 4.4 in [16].

Theorem 3: Given the SDE system (8) satisfying (H1)-(H2)-(H3). Let $\delta_0 \in \mathbb{R}_{\geq 0}$. Suppose that z is a random variable on $\mathbb{R}^n$ such that

$$\mathbb{E}[\|x_0 - z\|^2] \leq \delta_0^2.$$

Then, we have, for all $\tau \geq 0$:

$$\mathbb{E}[\sup_{0\leq t\leq\tau}\|X_{t,x_0} - \tilde{X}_{t,z}\|^2] \leq \delta^2_{\tau,\delta_0},$$

with $\delta^2_{\tau,\delta_0} := \beta(\tau)e^{\gamma\tau}$, where:

$$\begin{aligned}
&\gamma = 2(\sqrt{\Delta_t} + 2\lambda + L_g^2 + 128L_g^4), \text{ and}\\
&\beta(\tau) = 2\delta_0^2 + 2\tau\Delta_t L_g^2(1+128L_g^2)(F_{2,z}d + E_{2,z}\Delta_t)\\
&+ 4\tau\sqrt{\Delta_t}D(F_{4,z}d + E_{4,z}\Delta_t^2)^{\frac{1}{2}}\\
&(1+4\mathbb{E}\sup_{0\leq t\leq\tau}\|\underline{X}_{t,z}\|^{2q} + 4\mathbb{E}\sup_{0\leq t\leq\tau}\|\tilde{X}_{t,z}\|^{2q})^{\frac{1}{2}}.
\end{aligned} \tag{11}$$

with $\Delta_t = \tau/N$.