Guaranteed Overapproximations of Unsafe Sets for Continuous and Hybrid Systems: Solving the Hamilton-Jacobi Equation Using Viability Techniques*

Alexandre M. Bayen[1], Eva Crück[2], and Claire J. Tomlin[1]

[1] Hybrid Systems Laboratory, Stanford University, Stanford, CA
bayen@stanford.edu, tomlin@stanford.edu
[2] Laboratoire de Recherches Balistiques et Aérodynamiques, Vernon, France
eva.cruck@dga.defense.gouv.fr

Abstract. We show how reachable sets of constrained continuous and simple hybrid systems may be computed using the minimum time-to-reach function. We present an algorithm for computing a discrete approximation to the minimum time-to-reach function, which we prove to be a converging underapproximation to the actual function. We use the discrete minimum time-to-reach function for simple hybrid systems to compute overapproximations of unsafe zones for aircraft in a sector of the Oakland Air Traffic Control Center, leading to the automatic generation of conflict-free aircraft maneuvers.

1 Introduction

It is well known that verification of system safety may be achieved by computing the *reachable set of states*, that is, the set of all states from which the system has a trajectory which enters the set of unsafe states (or target). If the initial state of the system is outside of this set, then the safety property is verified. The design of methods to efficiently compute this set for continuous and hybrid systems remains a tough problem, though progress has been made for hybrid systems with linear or affine dynamics, or for which the set representation can be simplified to, for example, polyhedra or ellipsoids [1, 11, 6]. In previous work of Mitchell, Bayen, and Tomlin [16], we have performed this reachable set computation using a convergent approximation of a level set function $J(x,t)$, which is the solution of a time varying Hamilton-Jacobi Equation (HJE), such that $\{x \in \mathbb{R}^N : J(x,t) \leq 0\}$ is the set of states from which the system has a trajectory which reaches the target set $\{x \in \mathbb{R}^N : J(x,0) \leq 0\}$ in at most t time units.

In this paper, we consider the same reachability problem, using a different function to encode the reachable set: we define the *minimum time-to-reach function* $\theta_C^K(x)$ to be the minimum time for a trajectory of the system, starting at

* Research supported by DARPA under the Software Enabled Control Program (AFRL contract F33615-99-C-3014), by NASA under Grant NCC 2-5422, and by two Graduate Fellowships of the Délégation Générale pour l'Armement (France).

C.J. Tomlin and M.R. Greenstreet (Eds.): HSCC 2002, LNCS 2289, pp. 90–104, 2002.

state x, to reach the target set C while staying in a set K. The set of states from which the system has a trajectory which reaches the target set in at most t is thus $\{x \in \mathbb{R}^N : \theta_C^K(x) \leq t\}$. The minimum time-to-reach function has several interesting properties, which we will exploit here. First, the minimum time-to-reach function is known to exist and to be the unique Crandall-Evans-Lions viscosity solution ([12]) of a particular HJE (see Bardi [4]). Second, there exist numerical algorithms ([17, 10]) based on viability techniques (see Aubin [2, 3]) which compute guaranteed underapproximations of the minimum time-to-reach function, and therefore overapproximations of the reachable set, in the presence of constraints. These algorithms are based on discrete time, discrete state approximations of the continuous dynamics. Third, this function provides direct access to the "survival time" of the system within the reachable set, which is information that may readily be used for control purposes.

In this paper, we first define the minimum time-to-reach function in the context of both Hamilton-Jacobi equations and viability theory (set valued analysis). We present the first complete instantiation of an algorithm proposed by Saint-Pierre [18] in which we combine ideas from [8, 9] into a self-sufficient algorithm, which computes an underapproximation of this function. This algorithm actually computes the discrete minimum time-to-reach function for a discrete time, discrete state approximation of the continuous dynamics, whose trajectories we show to be "close", in a well-defined sense, to corresponding trajectories of the continuous dynamics. This discrete minimum time-to-reach function converges to the continuous minimum time-to-reach function as increments in the space and time step converge to zero: we generate proofs (inspired from [8, 9]) of well posedness and convergence. We provide a numerical validation of this algorithm by assessing its rate of convergence to the continuous function through two textbook examples (for which we know the continuous solution). In the second part of this paper, we consider the problem of maneuver synthesis in Sector 33 of the Oakland Air Traffic Control Center, which is one of the busiest sectors within this Center. We present an algorithm for computing the minimum time-to-reach function for hybrid and reset systems with one switch or reset. We then apply this algorithm to the generation of control policies for heading change or flight level change for sequences of aircraft.

Thus, the contributions of this paper are in the development and numerical implementation of a fast algorithm for computing a discrete underapproximation of the continuous minimum time-to-reach function, in the adaptation of the proofs of convergence of [8] to this special case, and in the extension of this method to the computation of guaranteed overapproximations of reachable sets for simple hybrid and reset systems (a recent previous extension has focussed on *impulse differential inclusions* [3]). Additional contributions are in the application of this algorithm to synthesizing safe maneuvers for aircraft in air traffic control. We show that the algorithms presented here, while less accurate than level set techniques, have advantages in the form of guaranteed set overapproximation, and survival time information.

2 Computing Reachable Sets of Continuous Systems

2.1 Reachability Using Minimum Time-to-Reach Functions

Let us consider the following control problem:

$$\begin{cases} \dot{x}(t) = f(x(t), u(t)), & t > 0 \\ x(0) = x \end{cases} \tag{1}$$

where $u(\cdot) \in \mathcal{U} := \{u : [0, +\infty[\rightarrow U, \text{ measurable}\}$ and U is a compact metric space, $x \in X = \mathbb{R}^N$, and f is continuous in u and Lipschitz-continuous in x. Following Aubin [2] we rewrite (1) in set valued form:

$$\begin{cases} \dot{x}(t) \in F(x(t)) \ := \{f(x, u)\}_{u \in U} \\ x(0) = x \end{cases} \tag{2}$$

The set of solutions of (2) (equivalently of (1)) is denoted $\mathcal{S}_F(x)$. Consider the following problem. Let $K \subset X$ be a constraint set and C be a closed set in K. Find the set of initial conditions x for which there exists a trajectory starting at x remaining in K and reaching C in finite time. In mathematical terms, we seek

$$W_C^K = \{x \in K : \exists x(\cdot) \in S_F(x), \exists t \geq 0, x(t) \in C \wedge (\forall s < t, x(s) \in K)\} \tag{3}$$

We define the minimum time-to-reach function as:

$$\theta_C^K(x) = \inf_{x(\cdot) \in S_F(x)} \inf\{t \in \mathbb{R}^+ : \quad x(t) \in C \quad \wedge \quad (\forall s < t, \ x(s) \in K)\} \tag{4}$$

Note that $\theta_C^K(x) = +\infty$ if all the trajectories originating at x leave K before reaching the target, or stay in K forever without reaching C.

Fact 1 *W_C^K may be computed using the minimum time-to-reach function:*

$$W_C^K = \text{Dom}\left(\theta_C^K\right) := \{x \in K : \theta_C^K(x) < +\infty\} \tag{5}$$

where Dom $(\cdot)$ *denotes the domain of definition of the function θ_C^K, or the set of points at which it is defined (here that is the set of points at which it is finite).*

2.2 Viscosity Solution of the Reachability Problem Using Viability

The minimum time-to-reach function $\theta_C^{\mathbb{R}^N}$ defined by (4) for (1) or (2) is known to be the viscosity solution of the following HJE (Bardi [4]):

$$\begin{cases} H(x, D\theta_C^{\mathbb{R}^N}) = 1 \text{ in } \Omega \backslash C \\ \theta_C^{\mathbb{R}^N} = 0 \qquad\quad \text{in } \partial C \\ \theta_C^{\mathbb{R}^N}(x) \rightarrow +\infty \quad \text{as } x \rightarrow \partial\Omega \end{cases} \tag{6}$$

where $\Omega \supset C$ is an open set. Note that the proofs of Bardi [4] hold when there are no constraints, i.e. $K = X = \mathbb{R}^N$ here, and under local controllability assumptions. For a more general Hamilton-Jacobi framework, see Frankowska [13]. The Hamiltonian of the system is given by: $H(x, p) = \max_{u \in U}\{-p \cdot f(x, u)\}$. The function θ_C^K can also be characterized with the help of the *viability kernel* of an extended dynamics of our original system (see [10] for more details):

Definition 1. *For set-valued dynamics*[1] $F : X \rightsquigarrow X$ *and a set* $K \subset X$*, we define the* viability kernel *of* K *as:*

$$\mathrm{Viab}_F(K) = \{x \in K : \exists x(\cdot) \in S_F(x),\ \forall t \geq 0 \quad x(t) \in K\} \tag{7}$$

Intuitively, the viability kernel is the set of points for which there exists a solution to (2) staying in K forever. The following can be found in [9]:

Proposition 1. *Assume that in (2),* F *is uppersemicontinuous*[2] *with compact convex nonempty values and that* K *and* C *are closed. Then*

$$\mathrm{Epi}\left(\theta_C^K\right) = \mathrm{Viab}_\Phi\left(K \times \mathbb{R}^+\right) \tag{8}$$

where $\mathrm{Epi}\left(\theta_C^K\right) := \{(x, y) \in K \times \mathbb{R}^+ : y \geq \theta_C^K(x)\}$ *denotes the epigraph of the function* θ_K^C*, i.e. the set of points above its graph, and where*

$$\Phi(x) = \begin{cases} F(x) \times \{-1\} & \text{if } x \notin C \\ \overline{\mathrm{co}}\{F(x) \times \{-1\}, \{0, 0\}\} & \text{if } x \in C \end{cases} \tag{9}$$

In (9), $\overline{\mathrm{co}}$ denotes the closure of the convex hull of the set between brackets (i.e. the closure of the smallest convex set containing it). Proposition 1 states that the set of points above the graph of the minimum time to reach function is the set of initial states $(x, y) \in K \times \mathbb{R}^+$ such that the trajectories $(x(\cdot), y(\cdot)) \in \mathcal{S}_\Phi((x, y))$ reach $C \times \mathbb{R}^+$ in finite time. Even if we do not make direct use of (7,8,9) in the present paper, they have proved crucial in the development of the techniques used here. Indeed, Proposition 1 links the minimum time-to-reach function to the viability kernel and therefore enables the use of the *viability kernel algorithm* (Frankowska and Quincampoix [14]) whose numerical implementation (Saint-Pierre [17]) provides a guaranteed overapproximation of $\mathrm{Epi}\left(\theta_C^K\right)$. In subsequent work, Cardaliaguet and al. [8] tailored the viability kernel algorithm to the computation of the minimum time-to-reach function. In [18], Saint-Pierre proposes a further simplification this algorithm. In the next section, we present our numerical algorithm inspired by [18].

2.3 Approximation Algorithm

We present a proof of the convergence of the *underapproximation algorithm* for the minimum time-to-reach function under state constraints, θ_C^K, adapted from [9, 18] for our design. The inclusion of state constraints will allow us to ignore the problem of boundary conditions. It gives good insight into the approximation procedure: the algorithm computes the exact minimum time-to-reach function for a discrete time dynamics defined on a discrete state space. Hence, we begin by showing how we can define a fully discrete dynamics whose trajectories are *good* approximations of the trajectories of system (2) (in a sense that will be defined).

[1] In the sequel, we shall use the arrow $\rightsquigarrow$ for "set valued" maps.

[2] A set valued map $F : X \rightsquigarrow X$ with compact values is uppersemicontinuous iff $\forall x_0 \in X$, and $\forall \varepsilon > 0$, $\exists \eta > 0$ such that $\forall x \in x_0 + \eta\mathcal{B}$, $F(x) \subset F(x_0) + \varepsilon\mathcal{B}$.

Numerical Approximation of Continuous Dynamics. We endow X with the Euclidean norm $\|\cdot\|$, and we denote by $\mathcal{B}$ the unit ball under this norm. For $h > 0$, we set $X_h = \left(h\mathbb{N}/\sqrt{2}\right)^N$, where $\mathbb{N}$ is the set of natural numbers. Then $\forall x \in X$, $\exists x_h$ in the ball $x + h\mathcal{B}$. Hence, X_h is a discrete approximation of the state space X. The following theorem defines approximations of $S_F(x)$ of the system (2) by the set of trajectories $S_\Gamma(x_h)$ of discrete dynamics $\Gamma : X_h \rightsquigarrow X_h$.

Theorem 1 (Relationship between continuous and discrete trajectories). *Assume that $F : X \rightsquigarrow X$ is upper semicontinuous with nonempty convex compact values and is l-Lipschitz. Assume moreover that there exists $M > 0$ such that for all $x \in K$, $\sup_{y \in F(x)} \|y\| \leq M$. For a mesh $h > 0$ and a time step $\rho > 0$, we define discrete dynamics on X_h:*

$$x_h^{n+1} \in \Gamma_{\rho,h}(x_h^n) := [x_h^n + \rho\,(\,F(x_h^n) + r(\rho,h)\mathcal{B}\,)] \cap X_h, \tag{10}$$

where $r(\rho,h) = lh + Ml\rho + 2\frac{h}{\rho}$, and we define the set of trajectories of this system as $S_{\Gamma_{\rho,h}}(x_h)$. Then a trajectory $x(\cdot)$ of system (2) defines trajectories of system (10) in the following way:

$$\forall \{x_h^n\} \in \{\{y_h^n\} : \forall n \in \mathbb{N},\ y_h^n \in (\,x(n\rho) + h\mathcal{B}\,)\}\,, \qquad \{x_h^n\} \in S_{\Gamma_{\rho,h}}(x_h), \tag{11}$$

and a trajectory $\{x_h^n\} \in S_{\Gamma_{\rho,h}}(x_h)$ is close to a trajectory $x(\cdot) \in S_F(x_h)$ in the following sense: $\forall t \geq 0$

$$\|x(t) - \hat{x}(t)\| \leq \begin{cases} \left(\,(\,M + r(\rho,h)\,)\,\rho + \frac{r(\rho,h)}{l}\right)(\mathrm{e}^{lt} - 1) & \text{if } l > 0 \\ 2\,\frac{h}{\rho}\,t & \text{if } l = 0 \end{cases} \tag{12}$$

where $\hat{x}(t) = x_h^n + \frac{x_h^{n+1} - x_h^n}{\rho}\,(t - n\rho)$, for $n \in \mathbb{N}$ and $t \in [n\rho, (n+1)\rho]$, represents a continuous trajectory interpolating points in $\{x_h^n\}$.

Proof: Please see Appendix. This theorem states that for all ρ and h, the dynamics (10) is an *overapproximation* of dynamics (2) in the following sense: all trajectories of system (2), when discretized with time step ρ and projected on X_h, are trajectories of (10); and all the trajectories of (10), when interpolated as in $\hat{x}(t)$ above, are approximations of trajectories of (2), with an upper bound on the error given by an increasing function of $\eta(\rho,h)$ (with $\eta(\rho,h) = 2h/\rho$ if $l = 0$) and of time. Therefore, the smaller the $\eta(\rho,h)$, the better the approximation. Moreover, $\eta(\rho,h)$ tends to 0 if and only if ρ, h and h/ρ tend to 0. This will be used in the approximation algorithm for the minimum time-to-reach function.

Approximation of the Minimum Time-to-Reach Function. We shall now define a fully discrete target problem which approximates the target problem defined for continuous time and state space, and shall prove relationships between the discrete minimum time-to-reach function and the continuous one. We shall use Θ to denote the discrete approximation of θ_C^K, its sub/superscripts will depend on context (and will always correspond to the sub/superscripts of θ).

We begin by defining a discrete approximation, and the sense in which discrete functions can converge to continuous functions.

Definition 2. *We say that a discrete function $\Psi_h : X_h \to \mathbb{R}$ is an* underapproximation *of a function $\theta : X \to \mathbb{R}$ if*

$$\forall x_h \in X_h, \quad \forall x \in (x_h + h\mathcal{B}), \qquad \Psi_h(x_h) \leq \theta(x),$$

and for a family (or a sequence) indexed by the set Ξ (containing elements called ξ) denoted $\{\Psi_{h,\xi}\}$, we write $\lim_{(h,\xi)\to(0^+,\xi_0)} \Psi_{h,\xi} = \theta$ if

$$\forall x \in X, \quad \lim_{(h,\xi)\to(0^+,\xi_0)} \sup_{x_h \in (x+h\mathcal{B})\cap X_h} \Psi_{h,\xi}(x_h) \;=\; \theta(x).$$

If moreover $\{\Psi_{h,\xi}\}$ is a underapproximation of θ for all $h > 0$ and all $\xi \in \Xi$, we say that it defines a converging underapproximation scheme of θ.

Theorem 2 (Discrete function is converging underapproximation of continuous). *Let $K \subset X$ be a closed set of constraints and $C \subset X$ be a closed target. Under the assumptions and notations of Theorem 1 and for $\rho > 0$ and $h > 0$, we denote $C_{\rho,h} = (C + (M\rho + h)\mathcal{B}) \cap X_h$ and $K_h = (K + h\mathcal{B}) \cap X_h$, and we define the discrete minimum time-to-reach function:*

$$\Theta^{K_h}_{C_{\rho,h}}(x_h) = \inf_{\{x_h^n\} \in S_{\Gamma_{\rho,h}}(x_h)} \inf\{n \in \mathbb{N} : x_h^n \in C_{\rho,h} \wedge \forall m < n,\, x_h^m \in K_h\} \quad (13)$$

Then $\left\{\Theta^{K_h}_{C_{\rho,h}}\right\}$ defines a converging underapproximation scheme of θ^K_C.

Corollary 1. *The minimum time-to-reach function θ^K_C can be underapproximated with use of a discrete function Θ^n, using the following algorithm:*

$$\Theta^0(x_h) = \begin{cases} 0 & \text{if } \; x_h \in K_h, \\ +\infty & \text{else} \end{cases} \quad (14)$$

$$\Theta^{n+1}(x_h) = \begin{cases} 1 + \inf_{y_h \in \Gamma(x_h)} \Theta^n(y_h) & \text{if } \; x_h \notin C_{\rho,h}, \\ \Theta^n(x_h) & \text{else} \end{cases} \quad (15)$$

Indeed, $\Theta^{K_h}_{C_{\rho,h}}(x_h) = \lim_{n\to+\infty} \Theta^n(x_h)$.

Proof of Theorem 2: Please see Appendix. The algorithm above provides a guaranteed underapproximation of the minimal time-to-reach function θ^K_C. The choice of the two parameters ρ and h is a matter of trial and error. However, when one of them is fixed, an interesting hint for setting the other is to minimize either $r(\rho, h)$ or $\eta(\rho, h)$ which appear in Theorem 1 and are indicators of the accuracy of the approximation by $\Gamma_{\rho,h}$.

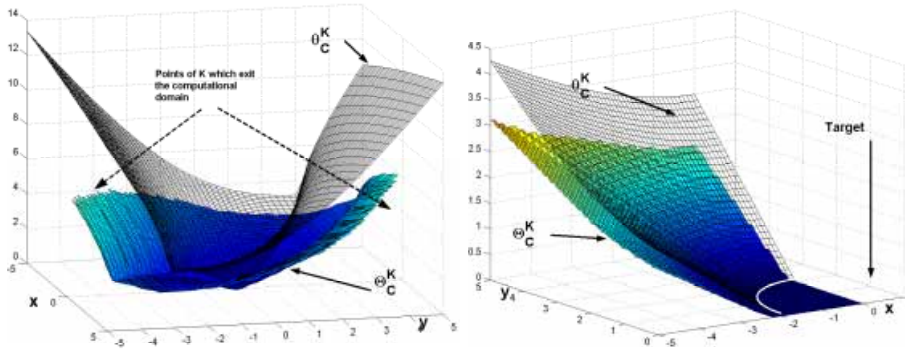

Fig. 1. Left: Numerical underapproximation of the value function of the double integrator problem (16), obtained by the the scheme presented in this paper. Computation realized on a 400 × 400 grid on $[-5, 5] \times [-5, 5]$, converged in 56 iterations, $\rho = 0.09$. **Right:** Numerical underapproximation of the value function of the wall pursuit evasion game (17). Computation realized on a 200 × 200 grid on $[-5, 0] \times [0, 5]$, converged in 36 iterations, $\rho = 0.09$. In both cases, three points out of four omitted in the plot for clarity. The numerical underapproximation of (17) is more accurate than that of (16). This is due to the zero Lipschitz constant of the dynamics of (17).

2.4 Numerical Validation

The previous section provides theoretical bounds for the error of the numerical approximation. However, as in Mitchell and al. [16], we need to assess how fast the method converges within these bounds.

Steering Problem (after Bryson [7]). The dynamical system for this problem is: $(\dot{x}, \dot{y}) = (y, u)$ where $u \in [-1, 1]$, $(x, y) \in \mathbb{R}^2$. The viscosity solution $\theta^{\mathbb{R}^2}_{(0,0)}$ of (6) corresponding for this dynamics is given by:

$$\begin{cases} \theta^{\mathbb{R}^2}_{(0,0)}(x, y) = -y + \sqrt{2y^2 - 4x} \text{ if } x + \frac{1}{2}y|y| \leq 0 \\ \theta^{\mathbb{R}^2}_{(0,0)}(x, y) = +y + \sqrt{2y^2 + 4x} \text{ if } x + \frac{1}{2}y|y| \geq 0 \end{cases} \tag{16}$$

The numerical results obtained from the underapproximation algorithm are compared to the viscosity solution $\theta^{\mathbb{R}^2}_{(0,0)}$ in Figure 1 (left). Clearly, the numerical result is below the analytical. The error is due to the Lipschitz constant of this example as related back to (12). We note here that Saint-Pierre [17] has developed powerful techniques to alleviate this problem.We did not implement them: they are computationally expensive and our goal here is fast overapproximations.

Wall pursuit evasion game (after Isaacs [15]). We treat this problem as a control problem by forcing the evader to run in one direction and reducing the space to the one quadrant. In this context: $(\dot{x}, \dot{y}) = (-w \cos d, \text{sign}(y) - w \sin d = 1 - w \sin d)$ with $(x, y) \in \mathbb{R}^- \times \mathbb{R}^+$: The pursuer has speed $w > 1$ and can move any direction d. Isaacs' *retrograde path equations* method enables reducing this problem to solving $(l + w\theta(x, y))^2 = x^2 + (y + \theta(x, y))^2$, which provides the

viscosity solution (17) of equation (6), shown in Figure 1 (right), as well as its numerical underapproximation obtained with our algorithm.

$$\theta^{\mathbb{R}^- \times \mathbb{R}}_{B(0,l) \cap \mathbb{R}^- \times \mathbb{R}}(x,y) = \frac{1}{w^2-1}\left[-(lw-|y|) + \sqrt{(|y|w-l)^2 + (w^2-1)x^2}\right] \quad (17)$$

3 Application to Safety Analysis of Air Traffic Control

3.1 Conflict Resolution in Heavily Loaded Air Traffic Centers

We are interested in performing fast computations of safety zones of aircraft for Air Traffic Management systems. Guaranteed underapproximation of those sets is crucial: certification of a conflict resolution protocol always requires a proof of its safety. We will here show the application of our technique to aircraft conflict resolution problems very frequently encountered in the Sector 33 airspace of the Oakland ATC Center in Fremont, CA. The computational example presented below is extracted from a larger modeling and control project which we are working on in collaboration with NASA Ames and with Oakland ATC Center [5]. For the present study, only a subset of this model is used.

Sector 33 is one of the busiest high altitude sectors in the US. It is at the junction of jetways coming from and going to Los Angeles, San Francisco, Oakland, San Jose, Las Vegas and is a collector of traffic from the east coast. At waypoint COALDALE in this sector, aircraft coming from Las Vegas may frequently conflict with aircraft going to the east coast at the same flight level (*floor*).

We consider the following subproblem (the notations refer to Figure 2). Let the local flight plan of aircraft 1 be jetway 92 towards COALDALE and then jetway 58 towards San Francisco, while the flight plan of aircraft 2 is jetway 58 through COALDALE . If the aircraft are in danger of "losing separation", meaning coming closer than 5 nautical miles horizontally and 2000ft vertically to each other, the controller will either reroute horizontally or climb one of the aircraft (i.e. will provide only one discrete action). The goal here is to develop advisories for air traffic controllers, so that aircraft do not lose separation.

Let $\boldsymbol{x}$ be the planar relative coordinate of the aircraft 1 w.r.t. aircraft 2, $\boldsymbol{v}_{92}$ the velocity vector of aircraft 1 along jetway 92, and $\boldsymbol{v}_{58}$ the velocity vector of aircraft 2 along jetway 58. We allow uncertainty in speed (due to winds, gusts, inaccuracy of sensors), with uncertainty bound of Mach $M = 0.05$.

$$\dot{\boldsymbol{x}} = \boldsymbol{v}_{58} - (\boldsymbol{v}_{92} + 0.05 \cdot c \cdot \mathcal{B}) \qquad \text{Mode 1} \quad (18)$$

where c is the speed of sound and $\mathcal{B}$ is the unit ball in $\mathbb{R}^2$. We can now apply the results of the previous section. Let us consider aircraft 1 as the evader and compute the safe set of its allowed positions (i.e. for which no loss of separation can occur). The unsafe set is the set of points which can eventually enter a disk target C around aircraft 2 of radius 5 nautical miles. Let us denote $\theta^{\text{mode 1}}$ the minimal time-to-reach function for target C (there are no state constraints here). Then the safe set is $\mathbb{R}^2 \setminus \text{Dom}\left(\theta^{\text{mode 1}}\right)$.

Conflict resolution via heading change (hybrid model).

A possible controller choice is to make aircraft 1 "cut" between jetway 92 and jetway 58. This avoids the conflict and shortens the path of aircraft 1, and is the preferred option of the controllers in general. This can be modeled as a second mode of aircraft 1, now rotated by an angle ψ to the west:

$$\dot{\boldsymbol{x}} = \boldsymbol{v}_{58} - R_\psi \cdot (\boldsymbol{v}_{92} + 0.05 \cdot c \cdot \mathcal{B}) \qquad \text{Mode 2} \tag{19}$$

where R_ψ is the standard rotation matrix of angle ψ. Let us denote $\theta^{\text{mode 2}}$ the minimal time function to reach C in this dynamics.

The controller's policy is the following: if aircraft 1 is safe in mode 1, stay in mode 1; else if it is safe in mode 2, switch to mode 2; if both modes are unsafe, switching can be used to increase the time during which the distance between the two aircraft is guaranteed to be greater than 5 nautical miles.

Denote by θ^{hybrid} the function representing the minimum guaranteed time before loss of separation, and by F_1 and F_2 the set valued dynamics associated to the two modes, and by $S_{F_1,F_2}(x,T)$ the set of trajectories originating at x for which switching from mode 1 to mode 2 occurs once. Then, at time T, we have:

$$\forall x \in X, \qquad \theta^{\text{hybrid}}(x) \;=\; \sup_{T>0} \inf_{x(\cdot)\in S_{F_1,F_2}(x,T)} \inf\{t>0 : x(t) \in C\} \tag{20}$$

with safe set $\mathbb{R}^2 \setminus \text{Dom}\left(\theta^{\text{hybrid}}\right)$. By definition, $\text{Dom}\left(\theta^{\text{hybrid}}\right) = \text{Dom}\left(\theta^{\text{mode 1}}\right) \cap \text{Dom}\left(\theta^{\text{mode 2}}\right)$ and $\forall x \in \mathbb{R}^2$, $\theta^{\text{hybrid}}(x) \geq \max\{\theta^{\text{mode 1}}, \theta^{\text{mode 2}}\}$. An algorithm for underapproximating θ^{hybrid} is presented in the next section.

Conflict resolution via floor climbing (reset model).

The second possible choice of the controller is to climb aircraft 1. It takes about 3 minutes to climb an aircraft from one floor to the next floor. If there are no aircraft on the next floor and there is enough time to climb the aircraft, then the problem is solved. Let us investigate the case in which there is another aircraft on the next floor (aircraft 3).

Let aircraft 1 be on floor 350 (35,000 ft) on jetway 92 towards COALDALE , aircraft 2 be on floor 350 on jetway 58 towards COALDALE and aircraft 3 on floor 370 (37,000) on jetway 58 towards COALDALE (see Figure 3). Given the positions of aircraft 2 and 3 on jetway 58 at their respective altitudes, we want to find the set of locations at which both collision cannot be avoided, and collision can be avoided by either climbing or staying at the same level. We assume that aircraft 2 and 3 are separated horizontally by a vector $\boldsymbol{\delta}$ (regardless of their altitude) and fly at the same speed (which is usually the case on high altitude jetways). If it takes T_{climb} seconds to climb from floor 350 to floor 370 and the horizontal speed during climbing is unchanged, let r be the following *reset function*:

$$r(\boldsymbol{x}) = \boldsymbol{x} + \boldsymbol{\delta} + T_{\text{climb}}\boldsymbol{v}_{92} \tag{21}$$

Then climbing aircraft 1 from floor 350 to floor 370 is equivalent to a reset. Let us call $\boldsymbol{x}$ the relative position of aircraft 1 w.r.t. aircraft 2: if $\theta(\boldsymbol{x}) < T_{\text{climb}}$, there is not enough time to climb aircraft 1 without causing loss of separation with

aircraft 2: the situation is unsafe. Otherwise, the aircraft can be climbed, and the algorithm in the next section will take this reset into account. Intuitively, the reset reinitializes the parameters by translating them by $\boldsymbol{\delta}$ plus $T_{\text{climb}}\boldsymbol{v}_{92}$, which is the ground distance needed to climb. As in the hybrid case, we will define θ^{reset} as the new minimal time-to-reach function which incorporates the possible reset within the execution of the automaton, and we will compute the set of points which are still unsafe when climbing is allowed, either because there is not enough time to climb, or the aircraft climbs to an unsafe zone on the next floor.

If we denote by $S_{F_1,r}(x,T)$ the set of trajectories originating at x for which resetting occurs at time T, we have

$$\forall x \in X, \qquad \theta^{\text{reset}}(x) = \sup_{T>0} \inf_{x(\cdot)\in S_{F_1,r}(x,T)} \inf\{t > 0 : x(t) \in C\} \tag{22}$$

and the safe set is $\mathbb{R}^2 \setminus \text{Dom}\,(\theta^{\text{reset}})$. An algorithm for underapproximating θ^{reset} is presented in the next section.

3.2 Computing Safe Sets for Hybrid and Reset Systems

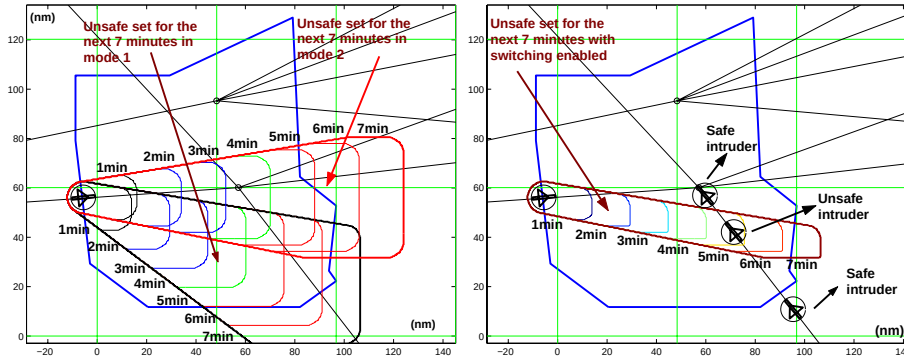

Fig. 2. Result of the conflict avoidance protocol with hybrid switching enabled. Computation realized on a 350 × 350 grid. **Left:** Reachability computation for the next 7 minutes for both modes (superimposed). Isolines are in increments of one minute in relative coordinates (which is why the distance between the isolines seems bigger than the one minute achievable distance of one aircraft at Mach $M = 0.85$ in absolute coordinates). If the intruder is in the intersection of the two unsafe sets, it cannot avoid loss of separation with the set of two maneuvers. If it is in one of the unsafe sets, switching avoids loss of separation. Otherwise, any of the two modes is safe. **Right:** Same as left with switching enabled. Position of first and third intruder are safe relative to these two dynamics. The second intruder cannot avoid loss of separation with only these two maneuvers.

Guaranteed underapproximation of the survival time function for the hybrid model. The algorithm presented below stems from Corollary 1

and provides an underapproximation of θ^{hybrid}. It is based on the fact that, given that the system starts in mode 1 and may switch to mode 2 at any time, $\theta^{\text{hybrid}}(x) = \theta^{\text{mode}\,2}(x)$ if $\theta^{\text{mode}\,2}(x) \geq \theta^{\text{mode}\,1}(x)$ because mode 2 guarantees safety longer than mode 1, otherwise $\theta^{\text{hybrid}}(x) \geq \theta^{\text{mode}\,1}(x)$ since mode 1 is safer now, and switching to mode 2 later may increase the time for which the system is safe.

Theorem 3 (Approximation of the hybrid minimum time-to-reach function). *Let $C \subset X$ be a closed target. We assume that F_1 and F_2 satisfy the assumptions of Theorem 1. For $\rho > 0$, $h > 0$ and $i \in \{1, 2\}$, we define the fully discrete dynamics $\Gamma^i_{\rho,h}$ and the discrete minimum time-to-reach functions $\Theta^{mode\,i}_{\rho,h}$ as in Theorems 1 and 2. Let $S_{\rho,h} := \{x_h \in X_h : \quad \Theta^{mode\,1}_{\rho,h}(x_h) \leq \Theta^{mode\,2}_{\rho,h}(x_h)\}$. Then a converging underapproximation scheme for θ^{hybrid} is given by $\Theta^{hybrid}_{\rho,h}(x_h) = \lim_{n\to+\infty} \Theta^n_{\rho,h}(x_h)$, where*

$$\begin{cases} \Theta^0_{\rho,h}(x_h) & = \sup\{\Theta^{mode\,1}_{\rho,h}(x_h), \Theta^{mode\,2}_{\rho,h}(x_h)\} \\ \Theta^{n+1}_{\rho,h}(x_h) & = \begin{cases} 1 + \inf_{y_h \in \Gamma^1_{\rho,h}(x_h)} \Theta^n_{\rho,h}(y_h) & \text{if} \quad x_h \notin S_{\rho,h} \\ \Theta^n_{\rho,h}(x_h) & \text{else} \end{cases} \end{cases} \tag{23}$$

Reset Models of Aircraft Climb. In the case of the reset model, the reasoning is similar to the hybrid case. Indeed, if a trajectory starts at x_0 with a reset at time T to x_1, we know that it cannot reach the target before $T + T_{\text{climb}} + \theta^{\text{mode}\,1}(x_1)$. In order to avoid loss of separation during climbing, we set

$$\theta^R(x) = \begin{cases} T_{\text{climb}} + \theta^{\text{mode}\,1}(r(x)) & \text{if } \theta^{\text{mode}\,1}(x) \geq T_{\text{climb}} \\ 0 & \text{else} \end{cases} \tag{24}$$

Then $\theta^R(x)$ plays the same role as $\theta^{\text{mode}\,2}$ in the hybrid model.

Theorem 4 (Approximation of the reset minimum time to reach function). *Let $C \subset X$ be a closed target. We assume that F satisfies the assumptions of Theorem 1 and that the reset function $r : X \to X$ is λ-Lipschitz continuous. For $\rho > 0$, $h > 0$, we define $\Gamma_{\rho,h}$ and the discrete minimum time-to-reach function $\Theta_{\rho,h}(x_h)$ as in Theorem 1. We also define the discrete reset function*

$$R_h(x_h) := (\ r(x_h) + (1+\lambda)h\mathcal{B}\ ) \cap X_h$$

Then a converging underapproximation scheme for θ^R is given by

$$\Theta^R_{\rho,h}(x_h) := \begin{cases} \inf_{y_h \in R_h(x_h)} \Theta^{mode\,1}_{\rho,h}(y_h) + \frac{T_{climb}}{\rho} & \text{if} \quad \Theta^{mode\,1}_{\rho,h}(x_h) \geq \frac{T_{climb}}{\rho}, \\ 0 & \text{else} \end{cases}$$

Furthermore, if $S_h := \{x_h \in X_h : \quad \Theta_{\rho,h}(x_h) < \Theta^R_{\rho,h}(x_h)\}$, then a converging underapproximation for θ^{reset} is given by $\Theta_{\rho,h}(x_h) = \lim_{n\to+\infty} \Theta^n(x_h)$, with

$$\Theta^0_{\rho,h}(x_h) = \sup\{\Theta_{\rho,h}(x_h), \Theta^R_{\rho,h}(x_h)\} \tag{25}$$

$$\Theta^{n+1}_{\rho,h}(x_h) = \begin{cases} 1 + \inf_{y_h \in \Gamma_{\rho,h}(x_h)} \Theta^n_{\rho,h}(y_h) & \text{if} \quad x_h \notin S_h, \\ \Theta^n_{\rho,h}(x_h) & \text{else} \end{cases} \tag{26}$$

Proofs of Theorems 3 and 4 are not included here, but are available from the authors.

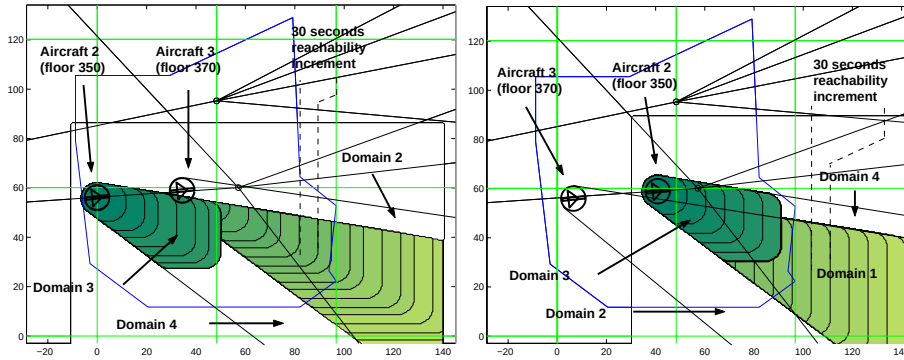

Fig. 3. Results of the conflict avoidance maneuver with reset enabled. Computation realized on a 350 × 350 grid with $T_{\text{climb}} = 3\text{min}$. Aircraft 2 and aircraft 1 are on floor 350. Aircraft 3 is on floor 370 approximately 35 miles ahead of (behind) aircraft 2. The different domains of the diagram have the following interpretation: if aircraft 1 is in Domain 1, there is no way conflict can be avoided by either climbing to 370 or staying on 350. If it is in Domain 2, it should stay there, for climbing will generate a conflict. In Domain 3, there is not enough time to climb, so conflict will occur on floor 350. In Domain 4, conflict can be avoided by climbing. Outside of these four domains, any altitude is safe. Each isoline represents a 30 sec. increment in the time to reach function w.r.t. the target (in relative dynamics).

4 Current Work

The version of our code used for the examples of this paper is designed in MATLAB. It is clear that the use of refinements proposed in [10] for the general viability kernel, such as local grid refinement and local Lipschitz constants, will improve the rate of convergence of the underapproximation algorithm. Yet even the simple code presented here provides guaranteed results, and its implementation for dimensions higher than 2, with reasonable computation time, should present few difficulties. In addition, while we have only presented the theorems for a single switch and reset here, we know the algorithm to be extendible to general hybrid systems, and we are currently working on this algorithm and proof.

References

[1] E. Asarin, O. Bournez, T. Dang, and O. Maler. Approximate reachability analysis of piecewise-linear dynamical systems. In B. Krogh and N. Lynch, editors, *Hybrid Systems: Computation and Control*, LNCS 1790, pages 21–31. Springer Verlag, 2000.

[2] J.-P. Aubin. *Viability Theory.* Systems & Control: Foundations & Applications. Birkhäuser, 1991.

[3] J.-P. Aubin, J. Lygeros, M. Quincampoix, S. Sastry, and N. Seube. Impulse differential inclusions: A viability approach to hybrid systems. Technical Report CUED/F-INFENG/TR.414, Department of Engineering - University of Cambridge, 2001.

[4] M. Bardi and I. Capuzzo-Dolcetta. *Optimal Control and Viscosity Solutions of Hamilton-Jacobi-Bellman Equations*. Birkäuser, 1997.

[5] A.M. Bayen, H. Sipma, C.J. Tomlin, and G. Meyer. Delay Predictive Models of The National Airspace System using Hybrid Control Theory: Design, Simulation and Proofs. *Proceedings of the American Control Conference*, 8-10 May 2002.

[6] O. Botchkarev and S. Tripakis. Verification of hybrid systems with linear differential inclusions using ellipsoidal approximations. In B. Krogh and N. Lynch, editors, *Hybrid Systems: Computation and Control*, LNCS 1790, pages 73–88. Springer Verlag, 2000.

[7] A.E. Bryson and Y.-C.Ho. *Applied Optimal Control,Optimization, Estimation and Control*. Taylor and Francis, 1975.

[8] P. Cardaliaguet, M. Quincampoix, and P. Saint-Pierre. Optimal Times for Constrained Nonlinear Control Problems without Local Controllability. *Applied Mathematics and Optimization*, 36:21–42, 1997.

[9] P. Cardaliaguet, M. Quincampoix, and P. Saint-Pierre. Numerical Methods for Differential Games. In M. Bardi, T.E.S. Raghavan, and T. Parthasarathy, editors, *Stochastic and Differential Games: Theory and Numerical Methods*, Annals of the International Society of Dynamic Games. Birkhäuser, 1999.

[10] P. Cardaliaguet, M. Quincampoix, and P. Saint-Pierre. Set-valued numerical analysis for optimal control and differential games. In M. Bardi, T.E.S. Raghavan, and T. Parthasarathy, editors, *Stochastic and Differential Games: Theory and Numerical Methods*, Annals of the International Society of Dynamic Games. Birkhäuser, 1999.

[11] A. Chutinan and B. H. Krogh. Approximating quotient transition systems for hybrid systems. In *Proceedings of the American Control Conference*, pages 1689–1693, Chicago, IL, 2000.

[12] M. G. Crandall, L. C. Evans, and P.-L. Lions. Some properties of viscosity solutions of Hamilton-Jacobi equations. *TransAMS*, 282(2):487–502, 1984.

[13] H. Frankowska. Lower Semicontinuous Solutions of Hamilton-Jacobi-Bellman Equations. *SIAM Journal of Control and Optimization*, 31(1):257–272, 1993.

[14] H. Frankowska and M. Quincampoix. Viability kernels of differential inclusions with constraints: Algorithm and applications. *Mathematics of Systems, Estimation and Control*, 1(3):371–388, 1991.

[15] R. Isaacs. *Differential Games*. Dover (reprint from John Wiley), 1999 (1965).

[16] I. Mitchell, A.M. Bayen, and C.J. Tomlin. Validating a Hamilton-Jacobi approximation to hybrid system reachable sets. In M.D. Di Benedetto and A. Sangiovanni-Vincentelli, editors, *Hybrid Systems: Computation and Control*, LNCS 2034, pages 418–432. Springer Verlag, 2001.

[17] P. Saint-Pierre. Approximation of the Viability Kernel. *Applied Mathematics and Optimization*, 29:187–209, 1994.

[18] P. Saint-Pierre. Approche ensembliste des systèmes dynamiques, regards qualitatifs et quantitatifs. *Matapli, Société de Mathématiques Appliquées et Industrielles*, 66, 2001.

Appendix

Proof — [Theorem 1 - adapted from [10]]. In order to prove the first part, let $x_0 \in X$ and $x(\cdot) \in S_F(x_0)$. We claim that $x((n+1)\rho) \in G_\rho(x(n\rho))$ for all $n \in \mathbb{N}$. Indeed, $x((n+1)\rho) = x(n\rho) + \int_{n\rho}^{(n+1)\rho} \dot{x}(t)dt$ and since F is l-Lipschitz, and bounded by M, we have $\forall n \in \mathbb{N}, \quad \forall t \in [n\rho, (n+1)\rho], \quad \dot{x}(t) \in F(x(t)) \subset F(x) + Mlt\,\mathcal{B}$. Furthermore, G_ρ is $(1+l\rho)$-Lipschitz. Hence,

$$\forall n \in \mathbb{N}, \quad \forall x_h^n \in (\, x(n\rho) + h\mathcal{B}\,) \cap X_h, \quad G_\rho(x(n\rho)) \;\subset\; G_\rho(x_h^n) + (1+l\rho)h\mathcal{B}$$

which completes the proof of the first part. We shall now prove the second part. Let $n \in \mathbb{N}$ and $t \in [n\rho, (n+1)\rho]$. The definition of $\hat{x}$ yields

$$\dot{\hat{x}}(t) \in F(x_h^n) + r(\rho,h)\mathcal{B} \tag{27}$$

$$\hat{x}(t) \in x_h^n + (\|F(x_h^n)\| + r(\rho,h))(t - n\rho)\mathcal{B} \tag{28}$$

Now since F is l-Lipschitz, $F(x_h^n) \subset F(\hat{x}(t)) + l\,\|\hat{x}(t) - x_h^n\|\,\mathcal{B}$. Hence, (27) yields

$$\dot{\hat{x}}(t) \in F(\hat{x}(t)) + (l(M + r(\rho,h))(t - n\rho) + r(\rho,h))\,\mathcal{B} \tag{29}$$

Let us set $\eta(\rho,h) = l(M + r(\rho,h))\rho + r(\rho,h)$. We have proved that $\dot{\hat{x}}(t) \in F(\hat{x}(t)) + \eta(\rho,h)\mathcal{B}$ for all t. Thanks to a theorem of Filippov[3], we know that there exists a trajectory $x(\cdot) \in S_F(x_h)$ such that

$$\forall t \geq 0, \quad \|x(t) - \hat{x}(t)\| \leq \mathrm{e}^{lt}\left(\int_0^t \eta(\rho,h)\mathrm{e}^{-ls}ds\right) \leq \begin{cases} \eta(\rho,h)\frac{(\mathrm{e}^{lt}-1)}{l} & \text{if } l > 0 \\ 2\,\frac{h}{\rho}\,t & \text{if } l = 0 \end{cases} \tag{30}$$

which completes the proof. △

Proof — [Theorem 2 - adapted from [10]] In order to prove that $\Theta^{K_h}_{C_{\rho,h}}$ is an underapproximation of θ^K_C, let $x_h \in K_h$ and let $x_0 \in x_h + h\mathcal{B}$ such that $\theta^K_C(x_0) < +\infty$. We denote $x(\cdot)$ an optimal trajectory in $S_F(x_0)$ originating at x_0. Then by the first part of Theorem 1, we can find trajectories $\{x_h^n\} \in S_{\Gamma_{\rho,h}}(x_h)$ such that $x_h^n \in (x(n\rho) + h\mathcal{B}) \cap X_h$. Now if $\theta^K_C(x) \in [n\rho, (n+1)\rho]$, **then** $x_h^n \in C_{\rho,h}$, and $x_h^m \in K_h$ for all $m < n$, which yields $\theta^K_C(x) \geq \rho\Theta^{K_h}_{C_{\rho,h}}(x_h)$ for all ρ, h. Thus, $\limsup_{h,\rho,\frac{h}{\rho}\to 0} \rho\Theta^{K_h}_{C_{\rho,h}}(x_h) \leq \theta^K_C(x)$. Now define two sequences $h_k \to 0$ and $\rho_k \to 0$ such that $\frac{h_k}{\rho_k} \to 0$ and

$$\mathcal{T} := \lim_{k\to+\infty} \rho_k \Theta^{K_{h_k}}_{C_{\rho_k,h_k}}(x_{h_k}) = \liminf_{\rho,h,\frac{h}{\rho}\to 0} \rho\Theta^{K_h}_{C_{\rho,h}}(x_h).$$

We shall prove that $\mathcal{T} \geq \theta^K_C(x)$. To this purpose, set $C_k := C_{\rho_k,h_k}$, $K_k := K_{h_k}$, and $\Gamma_k := \Gamma_{\rho_k,h_k}$. We denote by $\{x_k\}$ optimal trajectories for the fully discrete target problems with parameter k. Now let $x_k(\cdot) \in S_F(x_{h_k})$ denote the closest trajectories

[3] A consequence of the Filippov Theorem (Aubin [2, p.170]) is that if a function $y : \mathbb{R} \to X$ is such that $\dot{y}(t) \in F(y(t)) + \delta(t)\mathcal{B}$ for all t, then $\forall x_0 \in X$, $\exists x(\cdot) \in S_F(x_0)$ such that $\|x(t) - y(t)\| \leq \mathrm{e}^{lt}\left(\|x_0 - y(0)\| + \int_0^t \delta(s)\mathrm{e}^{-ls}ds\right)$ for all t.

as in Theorem 1. There exists a subsequence (again denoted) $x_k(\cdot)$ which converges[4] to some $x(\cdot) \in S_F(x)$ uniformly on the compact subsets of $\mathbb{R}^N$. By definition

$$\forall k \in \mathbb{N},\ x_k(\rho_k N_{C_k}^{K_k}(x_{h_k})) \in C_k + (l\,(M + r(\rho_k, h_k))\,\rho_k + r(\rho_k, h_k))\,\frac{(\mathrm{e}^{l(\rho_k N_{C_k}^{K_k}(x_{h_k}))} - 1)}{l}$$

Since C is closed, we have $x(\mathcal{T}) \in C$. Moreover, the uniform convergence of $x^k(\cdot)$ to $x(\cdot)$ and the closedness of K ensures that $x(t) \in K$ if $t \leq \mathcal{T}$. Thus, $\limsup_{h,\rho,\frac{h}{\rho}\to 0}\ \rho\Theta_{C_{\rho,h}}^{K_h}(x_h) \leq \theta_C^K(x)$ and $\limsup_{h,\rho,\frac{h}{\rho}\to 0}\ \rho\Theta_{C_{\rho,h}}^{K_h}(x_h) \geq \theta_C^K(x)$, meaning that $\limsup_{h,\rho,\frac{h}{\rho}\to 0}\ \rho\Theta_{C_{\rho,h}}^{K_h}(x_h) = \theta_C^K(x)$, which completes the proof. △

[4] A consequence of Theorem 3.5.2 in [2, p.101] is that if a sequence of points y^n converges to y, then a sequence of trajectories $y^n(\cdot) \in S_F(y^n)$ admits a subsequence which converges to some $y(\cdot) \in S_F(y)$ uniformly on the compact subsets of $\mathbb{R}^+$.