Computer-assisted proofs of non-reachability for linear finite-dimensional control systems

Ivan Hasenohr, Camille Pouchol, Yannick Privat, Christophe Zhang

Computer-assisted proofs of non-reachability for linear finite-dimensional control systems

Ivan Hasenohr[*] Camille Pouchol[†] Yannick Privat[‡§] Christophe Zhang[¶]

March 27, 2024

Abstract

It is customary to design a controlled system in such a way that, whatever the chosen control satisfying the constraints, the system does not enter so-called unsafe regions. This work introduces a general computer-assisted methodology to prove that a given linear finite-dimensional control systems with compact constraints avoids a chosen unsafe set. Relying on support hyperplanes, we devise a functional such that the property of interest is equivalent to finding a point at which the functional is negative. Actually evaluating the functional first requires time-discretisation. We thus provide explicit, fine discretisation estimates for various types of matrices underlying the controlled problem. Second, computations lead to roundoff errors, which are dealt with by means of interval arithmetic. The control of both error types then lead to rigorous, computer-assisted proofs of non-reachability of the unsafe set. We illustrate the applicability and flexibility of our method in different contexts featuring various control constraints, unsafe sets, types of matrices and problem dimensions.

Keywords: linear control systems, controllability under constraints, computer-assisted proofs, interval arithmetic

AMS classification: 49M29, 49M25, 65G30, 34H05.

1 Introduction

This article is dedicated to the rigorous estimation of the reachable set associated to a constrained controlled linear system. More precisely, we are interested in guaranteeing that, at a given time $T > 0$, the controlled system cannot enter a prescribed *unsafe region*, whatever the choice of control satisfying the given constraints.

We consider the linear autonomous control system

$$\begin{cases} \dot{y}(t) = Ay(t) + Bu(t), \\ y(0) = y_0, \end{cases} \tag{$\mathcal{S}$}$$

where $y_0 \in \mathbb{R}^n$ and $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$.

[*]Université Paris Cité, FP2M, CNRS FR 2036, MAP5 UMR 8145, F-75006 Paris, France. (ivan.hasenohr@u-paris.fr).

[†]Université Paris Cité, FP2M, CNRS FR 2036, MAP5 UMR 8145, F-75006 Paris, France. (camille.pouchol@u-paris.fr).

[‡]Université de Lorraine, CNRS, Institut Elie Cartan de Lorraine, Inria, BP 70239 54506 Vandœuvre-lès-Nancy Cedex, France. (yannick.privat@univ-lorraine.fr).

[§]Institut Universitaire de France (IUF)

[¶]Université de Lorraine, CNRS, Institut Elie Cartan de Lorraine, Inria, BP 70239 54506 Vandœuvre-lès-Nancy Cedex, France (christophe.zhang@polytechnique.org).

Given $y_0 \in \mathbb{R}^n$, a closed convex set $\mathcal{Y}_f \subset \mathbb{R}^n$, a time horizon $T > 0$ and a compact set $\mathcal{U} \subset \mathbb{R}^m$, we investigate the ($\mathcal{U}$-)constrained reachability problem, i.e., the problem of determining if there exists a control $u \in E$ such that the solution to ($\mathcal{S}$) with control u satisfies $y(T) \in \mathcal{Y}_f$, under the additional constraint that $u(t) \in \mathcal{U}$ for a.e. $t \in (0,T)$. If such a control exists, we shall say that *$\mathcal{Y}_f$ is $\mathcal{U}$-reachable from y_0 in time T*.

Our aim is to develop a general, flexible and certifiable methodology, resting on numerical computations, to show that $\mathcal{Y}_f$ is not $\mathcal{U}$-reachable from y_0 in time T. Ultimately, the interested user should be able to provide all parameters A, B, T, y_0, $\mathcal{U}$ and $\mathcal{Y}_f$ and, whenever that is the case, be returned the mathematically certified assertion that $\mathcal{Y}_f$ is not $\mathcal{U}$-reachable from y_0 in time T.

1.1 State of the art

The notion of constraint-free controllability of autonomous linear systems dates back to Kalman's seminal works. Its generalisation to infinite-dimensional systems is more recent. For further details on these concepts, we refer to the review books [21, 9]. Since the 70's, but more specifically in recent years, several works have investigated the addition of further constraints, satisfied whether by the control itself, or by the controlled trajectory.

Some of these works are theoretical in nature, with a focus on unbounded contraints. Particular interest has been given to the problems of exact controllability by positive controls for reasons of physical relevance [5, 31, 11, 14, 26, 27, 22]. Attention was also paid to adding constraints on the controlled trajectory [23, 24, 10]. Unbounded (sparsity) constraints have also been considered [34, 28].

In this article, we focus on the implementation of a method for numerically certifying that a set of unsafe states is unreachable, for compact constraint sets. Our approach is specific to autonomous (time invariant) linear systems. Regarding more general dynamical systems, closely related questions have been addressed in the past: for instance, how to numerically approximate the reachable set at time T, or guarantee that computed trajectories will not meet a given set (called unsafe set)?

In finite dimension, several methods have been elaborated to provide approximations of the reachable set (see for example the recent survey [1]): among others, let us mention the use of Hamilton-Jacobi type equations [25, 8], the design of barrier functions for trajectories to avoid unsafe regions [29, 15], and set propagation [1]. Let us roughly describe each of these approaches.

In [25, 8], a backwards reachable set is characterised as the zero sublevel set of the viscosity solution of a Hamilton-Jacobi type partial differential equation, with important applications to the safety of automated systems. This is formally related to our approach, as we also characterise non-reachability by the existence of negative values for a certain numerical criterion. As we will see, in this paper the convexity of the reachable set and the linearity of the system allow us to exploit this characterisation to produce numerical certificates of non-reachability.

In [29, 15], the authors introduce the notion of barrier functions, appropriately defined from the system dynamics to ensure that trajectories do not enter an unsafe zone. An important element of these methods is that these certificates are valid for all positive times $t > 0$, a very strong property which is not required in other methods. Moreover, the computation of barrier certificates for a given systems remains a challenging problem, both theoretically and numerically.

Set propagation is a class of methods for computing a guaranteed overapproximation or underapproximation of the reachable set of continuous systems. Starting from the set of initial states, the idea is to iteratively and adequately propagate a sequence of sets according to the system dynamics [12], which are guaranteed to contain, or be contained in, the reachable set. Such an algorithm has been developed in [19, 18] for finite-dimensional compact convex constraints. An important hurdle is then the so-called *wrapping effect*, that is, the accumulation of computational errors. The crux of set propagation techniques is to circumvent this difficulty by using appropriate propagation formulae.

There exist other ways to over- or under-approximate reachable sets, which rely on geometric properties. In the special case of ellipsoidal constraint sets, we refer to [16, 17]. More generally, for compact convex constraints, the reachable set can be approximated from the outside using support functions [2].

While the above-mentioned works provide theoretical criteria for finite dimensions, the case of infinite dimensions remains largely open.

1.2 Methodology: non-reachability criterion and certification issues

Support functions. Throughout, finite-dimensional spaces $\mathbb{R}^n$, $\mathbb{R}^m$ will be endowed with the standard Euclidean inner products. If we have $C \subset H$ with H a Hilbert space, σ_C will denote the *support function* of C defined by

$$\forall x \in C, \quad \sigma_C(x) = \sup_{y \in C} \langle x, y \rangle.$$

Non-reachability by separation. By means of separating hyperplanes, we will establish a necessary and sufficient criterion for non-reachability, involving a suitably defined function $J : \mathbb{R}^n \to \mathbb{R} \cup \{+\infty\}$, in the following form:

$$(\exists p_f \in \mathbb{R}^n, \quad J(p_f) < 0) \qquad \Longleftrightarrow \qquad \mathcal{Y}_f \text{ is not } \mathcal{U}\text{-reachable from } y_0 \text{ in time } T. \tag{1}$$

The precise definition of J (together with Figure 1 to convey the corresponding intuition) will be given in Section 1.2, and involves the support functions $\sigma_{\mathcal{U}}$ and $\sigma_{\mathcal{Y}_f}$, which we assume to be known explicitly.

The proof of (1) is the object of Proposition 2. In the case where $p_f \in \mathbb{R}^n$ such that $J(p_f) < 0$ is found, we will say that p_f is a *dual certificate* (that $\mathcal{Y}_f$ is not $\mathcal{U}$-reachable from y_0 in time T).

Computer-assisted proof of non-reachability. In what follows, we will exploit this criterion by producing vectors that satisfy it numerically. This raises questions pertaining to the error propagation inherent to every numerical method. More precisely:

> *Certified approach for non-reachability.*
>
> - How can one evaluate the functional J, in order to exhibit an element $p_f \in \mathbb{R}^n$ satisfying property (1) numerically?
> - How can one then **certify** the numerical result, which implies non-reachability? That is, guarantee that it is not flawed by various numerical approximations?

In order to carry out these two steps, there will in turn be two main difficulties.

(i) We will not have access to J but only to proxies obtained by discretisation, which we generically denote J_{d}. Indeed, the definition of J involves an integral, and the solution to a linear ODE involving A^*, hence amounts to computing the matrix exponentials $t \mapsto e^{tA^*}$. When these are not known explicitly, we will resort to simple time discretisation schemes (implicit Euler, etc) and provide a **bound on the error in terms of discretisation parameters**. One key aspect of our approach is that these bounds must be derived with explicit constants.

(ii) All computations will lead to **round-off errors**, which must be accounted for. To that end, we will use a Matlab/Octave toolbox called INTLAB (INTerval LABoratory) [33]. This code, entirely written in Matlab, is an interval arithmetic library. It provides tools for performing numerical computations with arbitrary precision arithmetic.

All in all, if for a given $p_f \in \mathbb{R}^n$ one lets $E_\mathrm{d}(p_f)$ (for the discretisation errors) and $E_\mathrm{r}(p_f)$ (for the round-off errors), we will have

$$J(p_f) \in [J_\mathrm{d}(p_f) - E_\mathrm{d}(p_f) - E_\mathrm{r}(p_f), J_\mathrm{d}(p_f) + E_\mathrm{d}(p_f) + E_\mathrm{r}(p_f)]. \tag{2}$$

Hence, we will take advantage of the fact that if

$$J_\mathrm{d}(p_f) + E_\mathrm{d}(p_f) + E_\mathrm{r}(p_f) < 0,$$

then y_f is not $\mathcal{U}$-reachable from y_0 in time T.

Here we stress that the notion of **certification** we are concerned with has to do with the numerical part of our work. We prove a theoretical necessary and sufficient condition for non-reachability. For a given system, we can determine whether it is satisfied numerically. Certifying this part then makes this numerical result theoretically sound, thus producing a **computer-assisted proof**.

Connections to existing results.

- In this article, we focus on the non-reachability of a given unsafe set instead of approximating the reachable set. This allows us to proceed by duality, and consider the solution to a single backwards equation, thus circumventing the wrapping effect. However, in terms of the reachable set, we only know that it is contained in a certified half-space.
- Computing several such half-spaces, one would then obtain an intersection of these half-spaces, guaranteed to contain the reachable set, which is closely related to the methods presented in [16, 19, 18]. However, this approach to computing a polyhedron is computationally heavy.
- Separation arguments already appear in reachability analysis [16, 17, 19, 18, 2]. An important contribution we make is to recast it in terms of the sign of the function J, in such a way that interval arithmetic can be applied to certify the end result, a feature which seldom appears in the literature.
- A key aspect of our methodology is to return a dual certificate p_f that *certifies* the corresponding mathematical statement: consequently, any user having access to their own discretised version of the functional J with corresponding error estimates, can verify the result upon using interval arithmetic.

Extensions and perspectives. We make the assumption that the support functions $\sigma_\mathcal{U}$ and $\sigma_{\mathcal{Y}_f}$ are known exactly. If it were not the case, our approach could be extended provided that one has a procedure to numerically evaluate them, together with a way to control the corresponding error.

The approach we have developed can be adapted *mutatis mutandis* to non-autonomous linear systems of the form $\dot{x}(t) = A(t)x(t) + B(t)u(t)$. The price to pay lies in the error formulae, in which the exponential matrix e^{tA} is replaced by the resolvent associated with the function $A(\cdot)$. The resulting formulae would then be slightly less accurate than those we obtained.

In the same vein, the reachability criterion can be extended without effort to Hilbert spaces. This is why we expect our method to accommodate **infinite-dimensional linear control systems**, provided that the space discretisation errors be also estimated. This will be the subject of further work, focusing in particular on the heat equation.

Our work is concerned with non-reachability. The natural complementary question is that of reachability: can one provide certified methods to show that a target y_f (or more generally, a set $\mathcal{Y}_f$) is reachable? We intend to tackle this problem as well, using similar geometric ideas.

Finally, a more prospective research direction would be to generalise our approach to non-linear controlled systems. It is likely that the methodology will have to be thoroughly modified.

Outline of the article. In Section 2, we introduce the criterion J and specify the separation argument which allows us to recast the non-reachability property. Section 3 is concerned with numerical methods for calculating J, using several possible discrete versions. Their relevance is discussed depending on the information at hand about A and its matrix exponential, and in each case, we provide fully explicit error bounds. Finally, the whole Section 4 is devoted to numerical experiments. After specifying the methodology leading to computer-assisted proofs of non-reachability, we apply it to three examples, with variable dimensions and constraint sets. We present concrete statements, the proofs of which are computer-assisted according to our methodology.

2 Non-reachability by separation

2.1 Main result

Consider the linear autonomous control system

$$\begin{cases} \dot{y}(t) = Ay(t) + Bu(t), \quad t \in [0, T], \\ y(0) = y_0, \end{cases} \tag{$\mathcal{S}$}$$

where $y_0 \in \mathbb{R}^n$ and $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, with $u \in E := L^2(0, T; \mathbb{R}^m)$. Recall that the control constraint set $\mathcal{U}$ is assumed to be compact, and the unsafe set $\mathcal{Y}_f$ to be closed and convex.

According to Duhamel's formula, the solution to ($\mathcal{S}$) at the final time T writes

$$y(T) = e^{TA}y_0 + L_T u, \qquad \text{where} \qquad L_T u := \int_0^T e^{(T-t)A}Bu(t)\, dt.$$

Letting $L(H_1, H_2)$ stand for linear continuous operators between two Hilbert spaces H_1 and H_2, it is standard that L_T defines an operator in $L(E, \mathbb{R}^n)$. Its adjoint $L_T^* \in L(\mathbb{R}^n, E)$ is defined for $p_f \in \mathbb{R}^n$ by $L_T^* p_f(t) = B^* p(t)$, where p solves the backward adjoint equation.

$$\begin{cases} \dot{p}(t) + A^* p(t) = 0, \quad t \in [0, T] \\ p(T) = p_f, \end{cases} \tag{3}$$

As already mentioned, the key point of our approach rests upon the assertion (1), where J denotes the so-called *dual* functional defined by

$$\forall p_f \in \mathbb{R}^n, \qquad J(p_f) = \int_0^T \sigma_{\mathcal{U}}(L_T^* p_f(t))\, \mathrm{d}t + \sigma_{\mathcal{Y}_f}(-p_f) + \langle y_0, e^{TA^*} p_f \rangle. \tag{4}$$

Remark 1. *When $\mathcal{U}$ is convex, the functional J can be understood as a dual functional associated to a primal problem, in the sense of Fenchel-Rockafellar. More details are provided in Appendix A. This interpretation leads us to consider useful algorithms that perform a descent over J in order to find dual certificates, as explained in Section 4.*

The following result describes the crucial argument underpinning our method, which is illustrated by Figure 1.

Proposition 2. *There exists $p_f \in \mathbb{R}^n$ such that $J(p_f) < 0$ if and only if $\mathcal{Y}_f$ is not $\mathcal{U}$-reachable from y_0 in time T.*

Proof. Let $\mathcal{U}_T := \{u \in E,\, t \in (0, T),\ u(t) \in \mathcal{U}$ for a.e. $t \in (0, T)\}$. With this notation in place, $\mathcal{Y}_f$ is not $\mathcal{U}$-reachable from y_0 in time T if and only if $(\mathcal{Y}_f - e^{TA}y_0) \cap L_T\mathcal{U}_T = \emptyset$. Using the basic relation $\sigma_{C-\{y\}}(z) = \sigma_C(z) - \langle y, z\rangle$, we have

$$\sigma_{\mathcal{Y}_f - e^{TA}y_0}(-p_f) = \sigma_{\mathcal{Y}_f}(-p_f) + \langle e^{TA}y_0, p_f\rangle = \sigma_{\mathcal{Y}_f}(-p_f) + \langle y_0, e^{TA^*}p_f\rangle$$

As a result, the function J defined in (4) rewrites

$$J(p_f) = \int_0^T \sigma_{\mathcal{U}}(L_T^* p_f(t))\,\mathrm{d}t + \sigma_{\mathcal{Y}_f - e^{TA}y_0}(-p_f) = \sigma_{\mathcal{U}_T}(L_T^* p_f) + \sigma_{\mathcal{Y}_f - e^{TA}y_0}(-p_f),$$

where the interchange of integration and supremum is justified, see e.g. [32, Theorem 14.60].

Now assume that we have found p_f such that $J(p_f) < 0$. Then

$$\sigma_{\mathcal{U}_T}(L_T^* p_f) = \sup_{u \in \mathcal{U}_T} \langle u, L_T^* p_f \rangle = \sup_{u \in \mathcal{U}_T} \langle L_T u, p_f \rangle < -\sigma_{\mathcal{Y}_f - e^{TA}y_0}(-p_f) = \inf_{y_f \in \mathcal{Y}_f} \langle y_f - e^{TA} y_0, p_f \rangle,$$

showing that one cannot find $u \in \mathcal{U}_T$ and $y_f \in \mathcal{Y}_f$ such that $L_T u = y_f - e^{TA} y_0$ and hence that $\mathcal{Y}_f$ is not $\mathcal{U}$-reachable from y_0 in time $T > 0$.

Conversely, suppose that $\mathcal{Y}_f$ is not $\mathcal{U}$-reachable from y_0 in time T. Then, the set of reachable states (from 0 in time T), i.e., the set $L_T \mathcal{U}_T$, is compact and convex since $\mathcal{U}$ is compact (see e.g. [20, Section 2.2]). The set $\mathcal{Y}_f - e^{TA} y_0$ is closed and convex.

By assumption, these two sets do not intersect, hence we may strictly separate them: there exists $p_f \in \mathbb{R}^n \setminus \{0\}$ such that

$$\sigma_{\mathcal{U}_T}(L_T^* p_f) = \sup_{w \in L_T \mathcal{U}_T} \langle w, p_f \rangle < \inf_{y_f \in \mathcal{Y}_f} \langle y_f - e^{TA} y_0, p_f \rangle = -\sigma_{\mathcal{Y}_f - e^{TA}y_0}(-p_f)$$

which amounts to $J(p_f) < 0$. □

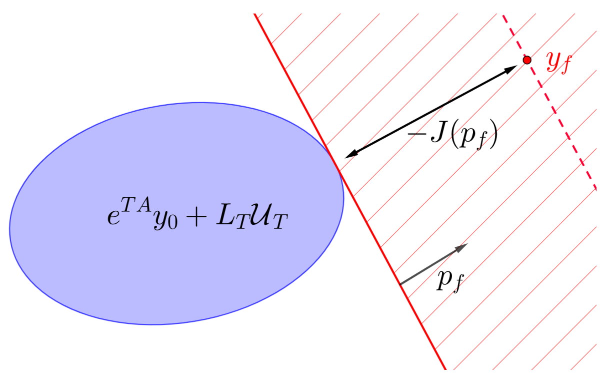

Figure 1: Reachable set $e^{TA}y_0 + L_T\mathcal{U}_T$, hyperplane associated to the dual certificate p_f, and corresponding scalar $J(p_f)$ given by (6), for a singleton $\mathcal{Y}_f = \{y_f\}$.

Remark 3. *By positive* 1*-homogeneity of support functions, J is also positively* 1*-homogeneous, meaning that $J(\lambda p_f) = \lambda J(p_f)$ for all $\lambda \geq 0$, $p_f \in \mathbb{R}^n$. In particular, if there exists p_f such that $J(p_f) < 0$, then $\inf_{p_f \in \mathbb{R}^n} J(p_f) = -\infty$.*

Remark 4. *We could also consider proving that $\mathcal{Y}_f$ is not $\mathcal{U}$-reachable from a full set of initial states $\mathcal{Y}_0 \subset \mathbb{R}^n$ in time T, in which case, defining*

$$\forall p_f \in \mathbb{R}^n, \qquad J(p_f) = \int_0^T \sigma_{\mathcal{U}}(L_T^* p_f(t))\,\mathrm{d}t + \sigma_{\mathcal{Y}_f}(-p_f) + \sigma_{\mathcal{Y}_0}(e^{TA^*} p_f)$$
$$= \int_0^T \sigma_{\mathcal{U}}(L_T^* p_f(t))\,\mathrm{d}t + \sigma_{\mathcal{Y}_f - e^{TA}\mathcal{Y}_0}(-p_f),$$

the result of Proposition 2 holds as is under the assumption that the set $\mathcal{Y}_f - e^{TA}\mathcal{Y}_0$ is closed and convex: this is the case for instance if $\mathcal{Y}_f$ is closed and convex, and $\mathcal{Y}_0$ convex and compact.

Remark 5. *The above proposition gives a necessary and sufficient condition for non-reachability. It is worth pointing out that, without any assumptions on the sets $\mathcal{U}$, $\mathcal{Y}_0$, $\mathcal{Y}_f$, the above criterion remains a sufficient condition for non-reachability, as it yields a strict separating hyperplane between $\mathcal{Y}_f$ and $e^{TA}\mathcal{Y}_0 + L_T\mathcal{U}_T$. In that case however, situations where these sets are disjoint but not separable by a hyperplane (typically if $\mathcal{Y}_f$ is not convex) are then undetectable by our approach.*

Remark 6. *As mentioned in the introduction, the above can be linked (at least formally) to the Hamilton-Jacobi characterisation of some reachable sets [25, 8]. Indeed, formally, in optimal control problems, the value function is a solution of a Hamilton Jacobi type equation. Now, for our control problem, the value function writes*

$$S(y_f) = \begin{cases} 0 & \textit{if } y_f \textit{ is reachable,} \\ +\infty & \textit{otherwise,} \end{cases}$$

so we see that the non-reachable set is characterised as the strict zero superlevel set $\{y,\ S(y) > 0\}$ of S. Note that S is a very singular function, and its numerical computation is not tractable, whereas a geometrical approach using support functions leads to a convex function on which a descent algorithm is then implemented, which is much more amenable and prone to numerical certification.

2.2 Unsafe sets and minimal times

As already mentioned, we throughout assume that we know an explicit formula for both functions $\sigma_{\mathcal{U}}$ and $\sigma_{\mathcal{Y}_f}$, which will be the case in the battery of examples we will provide. For instance, for $\mathcal{U}$ defined by the most standard box constraints $\ell_i \leq u_i \leq L_i$ for $i \in \{1, \dots, m\}$, one has with $\ell = (l_i)$, $L = (L_i)$ the explicit formula

$$\forall u \in \mathbb{R}^m, \quad \sigma_{\mathcal{U}}(u) = Lu_+ + \ell u_-, \tag{5}$$

where $u_+ = \max(u, 0)$ and $u_- = \min(u, 0)$ refer to the (componentwise) positive and negative parts of u respectively, and multiplications are to be understood componentwise.

Let us now discuss expressions for the functional (4) for some specific, yet natural, choices of sets $\mathcal{Y}_f$.

Chosen unsafe sets $\mathcal{Y}_f$. Most of our examples in this article will be based, but not limited to, the singleton case $\mathcal{Y}_f = \{y_f\}$. Below we compute the corresponding functional, and explain how one then infers results for a closed ball around y_f, *i.e.*, $\mathcal{Y}_f = \overline{B}(y_f, \varepsilon)$, and even a full half-space associated to y_f.

Section 4.3 features a more involved example where $\mathcal{Y}_f$ is a cylinder in $\mathbb{R}^4$, for the Space rendezvous problem.

Singleton. In the case $\mathcal{Y}_f = \{y_f\}$, one computes $\sigma_{\mathcal{Y}_f}(-p_f) = -\langle y_f, p_f\rangle$, which leads to the functional

$$J(p_f) = \int_0^T \sigma_{\mathcal{U}}(L_T^* p_f(t))\,\mathrm{d}t - \langle y_f, p_f\rangle + \langle y_0, e^{TA^*}p_f\rangle. \tag{6}$$

Ball. In the case of a ball $\mathcal{Y}_f = \overline{B}(y_f, \varepsilon)$ (which recovers the above case with $\varepsilon = 0$), we find

$$\sigma_{\mathcal{Y}_f}(-p_f) = -\langle y_f, p_f\rangle + \varepsilon\|p_f\|,$$

hence we uncover the same functional up to the additional term $\varepsilon\|p_f\|$.

In practice, this has the following implication: given y_f, assume that we have found p_f such that $J(p_f) < 0$ with J given by (6). Then $\overline{B}(y_f, \varepsilon)$ is not $\mathcal{U}$-reachable from y_0 in time $T > 0$ for any $\varepsilon < -J(\frac{p_f}{\|p_f\|})$. Hence, once a target y_f is fixed, we will only care with the functional J given by (6). If p_f is found such that $J(p_f) < 0$, we will obtain a full ball around y_f that is not $\mathcal{U}$-reachable from y_0 in time $T > 0$.

Half-space. Assume that $y_f \in \mathbb{R}^n$ is fixed, and let $\mathcal{Y}_f = \{y_f\}$. For the sake of this remark, when considering the associated functional (6), we highlight the dependence of J with respect to the target y_f, by writing $J(p_f; y_f)$ instead of $J(p_f)$.

Now assume that $\alpha := J(p_f; y_f)$ has been computed for a given $p_f \in \mathbb{R}^n$. For any $\tilde{y}_f \in \mathbb{R}^n$, we have the relation.

$$J(p_f; \tilde{y}_f) = J(p_f; y_f) + \langle y_f - \tilde{y}_f, p_f \rangle.$$

Hence, Proposition 1 shows that, independently of the sign of α, any vector in the half-space

$$\{\tilde{y}_f \in \mathbb{R}^n,\ \langle \tilde{y}_f - y_f, p_f \rangle > \alpha\},$$

is not $\mathcal{U}$-reachable from y_0 in time T. In other words, the computation of $J(p_f; y_f)$ for any p_f immediately provides a full half-space that is not $\mathcal{U}$-reachable from y_0 in time T.

Minimal times. It is interesting to notice that, still in the case where $\mathcal{Y}_f = \{y_f\}$ and assuming we have either $y_0 = 0$ or $y_f = 0$, we can also derive a lower bound on the minimum reachability time. We will exploit this result to provide minimum time estimates for various examples of controlled systems.

Proposition 7. *Assume that $\mathcal{U} \cap \mathrm{Ker}(B) \neq \emptyset$, and suppose either $y_0 = 0$ or $y_f = 0$.*

If y_f is not $\mathcal{U}$-reachable from y_0 in time T, then it is not reachable for any $\tilde{T} \leq T$ either. Consequently, denoting

$$T^\star(y_0, y_f, \mathcal{U}) = \inf\{T > 0,\ y_f \text{ is } \mathcal{U}\text{-reachable from } y_0 \text{ in time } T\} \in [0 + \infty],$$

we have $T^\star(y_0, y_f, \mathcal{U}) \geq T$.

Proof. This proposition is standard and its proof is elementary. Let us provide the main argument in the case where $y_0 = 0$ for the sake of completeness. Assume that y_f is $\mathcal{U}$-reachable from 0 in time $\tilde{T}$ by a control $\tilde{u}$. Let $T > \tilde{T}$. Let $v \in \mathcal{U} \cap \mathrm{Ker}B$. Then, the control u defined by $u(t) = v$ for $t \in (0, T - \tilde{T})$ and $u(t) = \tilde{u}(t - T + \tilde{T})$ steers the system from 0 to y_f in time T and satisfies the constraint, hence the conclusion. The end of the proof is straightforward. □

3 Discretisation and error estimates

This section gathers several discretisations and corresponding error estimates for the dual functional (4). Error estimates are given using standard Hermitian norms (over $\mathbb{C}^n$, $\mathbb{C}^m$), always denoted by $\|\cdot\|$. The same notation $\|\cdot\|$ will be used for the corresponding operator norms, that of matrices in $\mathbb{C}^{n\times n}$, $\mathbb{C}^{m\times n}$ or $\mathbb{C}^{n\times m}$.

As discussed in the introduction, we make the reasonable assumption that we have access to an explicit formula for $\sigma_{\mathcal{U}}$ (and $\sigma_{\mathcal{Y}_f}$). Also recall that $\mathcal{U}$ is compact, and M denotes a positive constant such that $\|v\| \leq M$ for all $v \in \mathcal{U}$.

3.1 Partial discretisation for a known adjoint exponential

In order to evaluate the dual functional (4) at a given point p_f, one is led to compute a time-integral, and to solve the backward equation (3). Given that $\sigma_{\mathcal{U}}$ will generally not be better behaved than Lipschitz, we will stick with time-discretisation schemes that are of order 1, whether for computing integrals or for integrating ODEs.

Even when one has access to an explicit solution for the backward equation (3), the integral will seldom be computable (or at the cost of cumbersome computations). This is why we first consider the case of discretising the integral but not the backward equation (3).

We let $N_t \in \mathbb{N}^*$, $\Delta t = T/N_t$, and for $k \in \{0, \dots, N_t\}$, $t_k = k\Delta t$. For a fixed $p_f \in \mathbb{R}^n$, we let $t \mapsto p(t)$ be the solution of (3), i.e., $p(t) = e^{(T-t)A^*} p_f$, and consider $J_{\mathrm{d},1}$, the first discretised version of J given by

$$J_{\mathrm{d},1}(p_f) = \Delta t \sum_{k=1}^{N_t} \sigma_{\mathcal{U}}(B^* p(t_k)) + \sigma_{\mathcal{Y}_f}(-p_f) + \langle y_0, p(0)\rangle. \tag{7}$$

Proposition 8. *For a given $p_f \in \mathbb{R}^n$, there holds*

$$|J(p_f) - J_{\mathrm{d},1}(p_f)| \leq \frac{1}{2}\Delta t\ MT\|B\| \Big(\sup_{t\in[0,T]} \|e^{tA^*}\|\Big) \|A^* p_f\|.$$

Proof. Recall that $\sigma_{\mathcal{U}}$ is M-Lipschitz continuous. Therefore, we have for all $s, t \in [0, T]$

$$|\sigma_{\mathcal{U}}(L_T^* p_f(s)) - \sigma_{\mathcal{U}}(L_T^* p_f(t))| \leq M\|B^* p(s) - B^* p(t)\| \leq M\|B\|\|p(t) - p(s)\|.$$

We may now bound

$$|\sigma_{\mathcal{U}}(L_T^* p_f(s)) - \sigma_{\mathcal{U}}(L_T^* p_f(t))| \leq M\|B\| \sup_{t\in[0,T]} \|A^* p(t)\|\|t - s\|.$$

We have proved that $t \mapsto \sigma_{\mathcal{U}}(L_T^* p_f(t))$ is Lipschitz continuous. Recalling the standard estimate

$$\left|\int_0^T f(t)\,\mathrm{d}t - \Delta t \sum_{k=1}^{N_t} f(t_k)\right| \leq \frac{1}{2} LT\,\Delta t$$

for a L-Lipschitz function $f : [0, T] \to \mathbb{R}$, we end up with

$$\left|\int_0^T \sigma_{\mathcal{U}}(B^* p(t))\,\mathrm{d}t - \Delta t \sum_{k=1}^{N_t} \sigma_{\mathcal{U}}(B^* p(t_k))\right| \leq \frac{1}{2}\Delta t MT\|B\| \sup_{t\in[0,T]} \|A^* p(t)\|,$$

and the announced estimate readily follows, using the definition of $p(t)$:

$$\begin{aligned}\sup_{t\in[0,T]} \|A^* p(t)\| &= \sup_{t\in[0,T]} \|A^* e^{(T-t)A^*} p_f\| = \sup_{t\in[0,T]} \|A^* e^{tA^*} p_f\| \\ &= \sup_{t\in[0,T]} \|e^{tA^*} A^* p_f\| \leq \sup_{t\in[0,T]} \|e^{tA^*}\|\|A^* p_f\|.\end{aligned}$$

□

Jordan-Chevalley decomposition. Even if one knows the matrix exponentials $t \mapsto e^{tA^*}$ (or equivalently the matrix exponentials $t \mapsto e^{tA}$), it remains to provide an upper bound for $\sup_{t\in[0,T]} \|e^{tA^*}\| = \sup_{t\in[0,T]} \|e^{tA}\|$ for the bound of Proposition 8 to be of any use.

Assume that we have access to the Jordan-Chevalley decomposition of A in the following sense: we have $A = D + N$ where D is diagonalisable, N is nilpotent with index ℓ, the two matrices D and N commute. Then, of course, e^{tA} is obtained by

$$\forall t \in \mathbb{R}, \qquad e^{tA} = e^{tD} \sum_{k=0}^{\ell-1} \frac{N^k}{k!} t^k = e^{tD} Q_\ell(tN), \tag{8}$$

where Q_ℓ is the polynomial $x \mapsto \sum_{k=0}^{\ell-1} \frac{x^k}{k!}$. Assume further that we have access to the transition matrix P that diagonalises D, i.e., $\mathrm{diag}(\Lambda) = P^{-1} D P$ where $\Lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{C}^n$ is the vector of eigenvalues of A.

Then, we have

$$e^{tA} = Pe^{t\Lambda}P^{-1}Q_\ell(tN),$$

which leads to the estimate

$$\sup_{t\in[0,T]} \|e^{tA}\| \leq \kappa(P)e^{\mu T}Q_\ell(\|N\|T),$$

where $\mu := \max(\{\mathrm{Re}(\lambda_i),\ i \in \{0,\dots,n\}\}$ is the spectral abscissa of A, and $\kappa(P) = \|P\|\|P^{-1}\|$ stands for the condition number of the transition matrix P.

From these estimates, we derive the error formula below, in the case where the Jordan-Chevalley decomposition is known.

Corollary 9. *Let us assume that the Jordan-Chevalley decomposition of A leads to the expression (8). Then for a given $p_f \in \mathbb{R}^n$, there holds*

$$|J(p_f) - J_{\mathrm{d},1}(p_f)| \leq \frac{1}{2}\Delta t\ MT\|B\|\|A^*p_f\|\kappa(P)e^{\mu T}Q_\ell(\|N\|T).$$

3.2 Full discretisation

Now we come to the case where the adjoint exponential $t \mapsto e^{tA^*}$ is not known, so that one needs to discretise the backward equation (3) as well. Assume that some discretisation scheme has been used, that produces $p_k \in \mathbb{R}^n$, for $k \in \{0,\dots,N_t\}$.

In the next subsection, we will specialise to the Euler implicit scheme for the class of negative semi-definite matrices.

The full discretised version of J then reads

$$J_{\mathrm{d},2}(p_f) = \Delta t \sum_{k=1}^{N_t} \sigma_{\mathcal{U}}(B^*p_k) + \sigma_{\mathcal{Y}_f}(-p_f) + \langle y_0, p_0\rangle. \tag{9}$$

Proposition 10. *For a given $p_f \in \mathbb{R}^n$ and vectors $p_k \in \mathbb{R}^n$, $k \in \{0,\dots,N_t\}$, there holds*

$$|J(p_f) - J_{\mathrm{d},2}(p_f)| \leq \Delta t\ M\|B\|\left(\frac{1}{2}T\|A^*p_f\|\sup_{t\in[0,T]}\|e^{tA^*}\| + \sum_{k=1}^{N_t}\|p(t_k) - p_k\|\right) + \|y_0\|\|p(0) - p_0\|.$$

The proof is straightforward and left to the reader, since all we have to do is provide an estimate for $|J_{\mathrm{d},1}(p_f) - J_{\mathrm{d},2}(p_f)|$ and combine it with the estimate given in Proposition 8.

We now discuss the application of the simplest possible scheme (again, recall that we are somewhat limited to schemes of order 1 since we are discretising the integral of a mere Lipschitz function), that is the Euler explicit scheme:

$$\begin{cases} p_{N_t} = p_f \\ p_k = (\mathrm{Id} + \Delta t A^*)p_{k+1} \quad \forall k \in \{0,\dots,N_t - 1\}. \end{cases} \tag{10}$$

Note that the Euler implicit scheme could be used and would lead to similar results. It is then standard (see e.g. [30, Section 11.3.2]) that

$$\forall k \in \{0,\dots,N_t\}, \quad \|p(t_k) - p_k\| \leq \frac{1}{2}\Delta t\ (T - t_k)\Big(\sup_{t\in[t_k,T]}\|p''(t)\|\Big)e^{\|A\|T},$$

which, given that $p''(t) = e^{(T-t)A^*}(A^*)^2p_f$, leads to the estimate

$$\forall k \in \{0,\dots,N_t\}, \quad \|p(t_k) - p_k\| \leq \frac{1}{2}\Delta t\ (T - t_k)\Big(\sup_{t\in[t_k,T]}\|e^{tA^*}\|\Big)e^{\|A\|T}\|(A^*)^2p_f\|$$

$$\leq \frac{1}{2}\Delta t\ (T-t_k)e^{2\|A\|T}\|(A^*)^2 p_f\| \tag{11}$$

We acknowledge that constants appearing in the above might slightly be improved.

All in all, we thus find following the global estimate.

Proposition 11. *For a given $p_f \in \mathbb{R}^n$ and vectors $p_k \in \mathbb{R}^n$, $k \in \{0,\dots,N_t\}$ defined according to the Euler explicit scheme (10), there holds*

$$|J(p_f) - J_{\mathrm{d},2}(p_f)| \leq \frac{1}{2}\Delta t\ T\left[M\|B\|\left(e^{\|A\|T}\|A^* p_f\| + \frac{1}{2}Te^{2\|A\|T}\|(A^*)^2 p_f\|\right) + \|y_0\|e^{2\|A\|T}\|(A^*)^2 p_f\|\right].$$

Proof. The only step that requires some details is the estimate for the sum of the errors $\|p(t_k) - p_k\|$, which is obtained by writing

$$\sum_{k=1}^{N_t}\|p(t_k) - p_k\| \leq \frac{1}{2}\Delta t\, e^{2\|A\|T}\|(A^*)^2 p_f\|\sum_{k=1}^{N_t}(T-t_k) = \frac{1}{2}\Delta t\, e^{2\|A\|T}\|(A^*)^2 p_f\|\frac{T}{N_t}\sum_{k=1}^{N_t}(N_t - k).$$

The sum $\sum_{k=1}^{N_t}(N_t-k)$ equals $\frac{(N_t-1)N_t}{2}$, hence

$$\sum_{k=1}^{N_t}\|p(t_k) - p_k\| = \frac{1}{4}\Delta t\, e^{2\|A\|T}\|(A^*)^2 p_f\| T(N_t - 1) \leq \frac{1}{4}T^2 e^{2\|A\|T}\|(A^*)^2 p_f\|.$$

□

This estimate has one major drawback: it diverges exponentially fast as a function of T, making the investigation of non $\mathcal{U}$-reachability challenging, even for moderate times $T > 0$, especially if the matrix norm $\|A\|$ is large.

3.3 Full discretisation for a symmetric negative semidefinite matrix

The purpose of this subsection is to exhibit a class of matrices, that of symmetric negative semidefinite matrices, for which refined estimates without exponentially diverging errors (as a function of time T) can be derived.

Even though such matrices are diagonalisable, computing their exponential can become intractable for large sizes, so that one needs to resort to discretisation for the backward equation (3). The implicit Euler scheme below is well suited to that situation:

$$\begin{cases} p_{N_t} = p_f \\ (\mathrm{Id} - \Delta t A^*)p_k = p_{k+1} \quad \forall k \in \{0,\dots,N_t - 1\}. \end{cases} \tag{12}$$

It always makes sense provided Δt is small enough, and in the case where the matrix A is a negative semidefinite symmetric matrix, the Euler implicit scheme is well-defined whatever the value of $\Delta t > 0$.

Assume we are given a symmetric positive semidefinite matrix C, diagonalised in the form $C = PDP^{-1}$, with D diagonal and P a orthogonal transition matrix, we may define $\varphi(C)$ for any function $\varphi : [0,+\infty) \to \mathbb{R}$ by $\varphi(C) = P\varphi(D)P^{-1}$ with componentwise application of φ on the diagonal. This definition obviously agrees with the usual matrix exponential and rational fractions whose poles avoid $[0,+\infty)$[1] Using that $\kappa(P) = 1$, one has for all such functions

$$\|\varphi(C)\| = \|\varphi(D)\| \leq \sup_{x\geq 0}|\varphi(x)|,$$

[1]There are of course much more general definitions for functions of matrices [13], but in the present setting this definition will suffice.

Proposition 12. *Assume that A is a negative semidefinite symmetric matrix, and let $p_f \in \mathbb{R}^n$. Then the error between the solution of the backward ODE (3) and its implicit Euler discretisation (12) satisfies*

$$\forall k \in \{0, \dots, N_t\}, \quad \|p(t_k) - p_k\| \le \frac{1}{2}\Delta t \, \|A^* p_f\|.$$

Proof. By definition, for all $k \in \{0, \dots, N_t\}$, we have

$$p(t_k) - p_k = \left[e^{(T-t_k)A^*} - (\mathrm{Id} - \Delta t A^*)^{-(N_t-k)}\right] p_f.$$

Hence me may write

$$p(t_k) - p_k = -\Delta t \, \varphi_{N_t-k}(-\Delta t A^*) A^* p_f,$$

where for $k \in \mathbb{N}^*$, the function φ_k is defined for $x > 0$ by

$$\varphi_k(x) = \frac{e^{-kx} - (1+x)^{-k}}{x},$$

extended by continuity at $x = 0$ by $\varphi_k(0) = 0$.

Estimating, we find

$$\|p(t_k) - p_k\| \le \Delta t \, \|\varphi_{N_t-k}(-\Delta t A^*)\| \, \|A^* p_f\| \le \Delta t \sup_{x \ge 0} |\varphi_{N_t-k}(x)| \|A^* p_f\|$$

Let us conclude by proving that $\sup_{x \ge 0} |\varphi_k(x)| \le \frac{1}{2}$ for all $k \ge 1$. First, a routine study shows that the function $x \mapsto e^{-x}(1+x) - 1 + \frac{1}{2}x^2$ is nonnegative for all $x \ge 0$, so that

$$|\varphi_1(x)| = \frac{1}{x}\left[\frac{1}{1+x} - e^{-x}\right] \le \frac{1}{2}x, \tag{13}$$

which combined with the basic estimate $|\varphi_1(x)| \le \frac{1}{x}\frac{1}{1+x}$ for $x > 0$ yields $|\varphi_1(x)| \le \frac{1}{2}$ by considering the two cases $x \le 1$ and $x > 1$. Now for $k \ge 2$, and $x > 0$, we write

$$|\varphi_k(x)| = \frac{1}{x}\left[\frac{1}{1+x}\right] \sum_{j=0}^{k-1} e^{-jx}\left(\frac{1}{1+x}\right)^{k-j-1} = |\varphi_1(x)| \sum_{j=0}^{k-1} e^{-jx}\left(\frac{1}{1+x}\right)^{k-j-1} \le |\varphi_1(x)| \frac{k}{(1+x)^{k-1}}.$$

thanks to the bound $e^{-x} \le \frac{1}{1+x}$. Let us focus on the case $k = 2$. If $x \le 1$, we have $|\varphi_2(x)| \le \frac{1}{2}x\frac{2}{1+x} \le \frac{1}{2}$, and for $x > 1$, $|\varphi_2(x)| \le \frac{1}{x(1+x)}\frac{2}{1+x} \le \frac{1}{2}$, hence the result for $k = 2$.

Now for any $k \ge 3$, using the estimate (13), we obtain the inequality

$$|\varphi_k(x)| \le \frac{kx}{2(1+x)^{k-1}}$$

The right-hand side is maximised at $\frac{1}{k-2}$, hence

$$|\varphi_k(x)| \le \frac{k}{2(k-2)}\left(\frac{k-2}{k-1}\right)^{k-1} = \frac{1}{2}\frac{k(k-2)}{(k-1)^2}\left(\frac{k-2}{k-1}\right)^{k-3} \le \frac{1}{2}.$$

□

This entails the following compact estimate for the dual functional.

Proposition 13. *Assume that A is a symmetric negative semidefinite matrix. For a given $p_f \in \mathbb{R}^n$ and vectors $p_k \in \mathbb{R}^n$, $k \in \{0, \dots, N_t\}$ defined according to the Euler implicit scheme (12), there holds*

$$|J(p_f) - J_{\mathrm{d},2}(p_f)| \le \Delta t \, \|A^* p_f\| \left(TM\|B\| + \frac{1}{2}\|y_0\|\right). \tag{14}$$

Proof. We simply build upon the general estimate of Proposition 10. First, we have the bound $\|e^{tA^*}\| \leq 1$ for all $t \geq 0$, and the previous estimate (12) for the Euler implicit scheme shows that

$$\sum_{k=1}^{N_t} \|p(t_k) - p_k\| \leq \frac{1}{2}\Delta t \|A^* p_f\| N_t = \frac{1}{2} T \|A^* p_f\|.$$

Remark 14. *We note that similar estimates, not exponentially diverging with T, could also be derived for the broader class of dissipative matrices (i.e., matrices A satisfying $\langle Ax, x\rangle \leq 0$ for all $x \in \mathbb{R}^n$).*

□

4 Numerical approach and examples

In this section, we will illustrate the potential of the approach described in the previous section to study the (non)-reachability of certain targets, in a variety of examples. We present three main example families, respectively related to:

- the control of a streetcar that we wish to control in order to reach a final state in minimum time. This is a well-known toy problem in optimal control theory. We use it to validate our results since the reachable set and minimal times (from $(0,0)^T$) have known explicit formulae;
- the spatial rendezvous problem. We want to use a control to reach a given target, corresponding to a space station, for instance the ISS, in a referential centered in the initial position of the spacecraft. We use a dynamic space mechanics model and provide certified lower-bounds on the minimal time needed to reach the target. We then develop a method to prove that a motionless obstable - e.g. an asteroid - cannot be collided with within a predetermined time interval.
- a more academic case, in which negative semi-definite Jacobi matrices A (of possibly large dimension) are randomly generated.

Most cases feature a set of the form $\mathcal{Y}_f = \{y_f\}$, hence the function of interest is (6). As explained in Subsection 2, the use of the corresponding functional also allows us to certify that balls around y_f or even half-spaces cannot be reached. The types of constraint sets $\mathcal{U}$ also vary across examples.

4.1 Numerical approach and methodology

In order to numerically verify the non $\mathcal{U}$-reachability of a given target y_f from y_0 in time T, one must proceed through the following three steps:

1. First, one must compute a discretisation J_{d} of the functional J, for example $J_{\mathrm{d},1}$ or $J_{\mathrm{d},2}$, with the associated bounds on discretisation errors
2. Then, one must minimise said discretisation in order to find an element p_f such that $J_{\mathrm{d}}(p_f) < 0$.
3. Finally, one must compute $e(p_f)$ such that $J_{\mathrm{d}}(p_f) - e(p_f) \leq J(p_f) \leq J_{\mathrm{d}}(p_f) + e(p_f)$. This is typically done using the INTLAB toolbox [33], which, using interval arithmetic, takes into account the rounding errors and added discretisation errors. This leads to the verification that indeed, $J(p_f) \leq J_{\mathrm{d}}(p_f) + e(p_f) < 0$. If that is not the case, either y_f is reachable, or a finer discretisation or minimisation is required to prove its non-reachability.

Since INTLAB allows for most of usual computation techniques, the second and third steps could be joined. However, interval arithmetic is computationally expensive, hence we first minimise the discretised functional J_{d} to find p such that $J_{\mathrm{d}}(p_f) < -\eta$, where η is the typical size of errors $e(p_f)$ (on the ball $\|p_f\| = 1$), and then verify that p_f is indeed a certificate of non $\mathcal{U}$-reachability for y_f. Since this stopping condition will never be satisfied if the target set $\mathcal{Y}_f$ is in fact $\mathcal{U}$-reachable, one might consider adding another condition based on how small an improvement is made from one step to another. As the functional J_{d} may not have a minimiser (see Remark 3), we use the stopping condition

$$\left| \frac{p_{k+1}}{\|p_{k+1}\|} - \frac{p_k}{\|p_k\|} \right| \leq \delta,$$

where δ is chosen to be small.

Minimising J_{d} can be tackled by means of many optimisation techniques. For the following examples, we take advantage of the dual nature (see Appendix A) of the problem with the choice of functions (23), assuming $\mathcal{U}$ is convex. This allows us to use the Chambolle-Pock primal-dual algorithm [6]. It has the drawback of requiring a closed-form expression of two proximal operators associated with the functionals F^* and G, as defined in Appendix A. In general, if $\sigma_{\mathcal{U}}$ and $\sigma_{\mathcal{Y}_f}$ have closed-form formulae, so do those proximal operators.

4.2 The streetcar

Control problem. The following example is completely standard in optimal control theory. It can be found for example in [20, Chapter 1] and is concerned with the optimal control of the acceleration of a streetcar on a straight axis, in order to reach a stop station at zero speed.

We will use this example to both illustrate and to validate our approach, since the reachable set and minimal times are known explicitly, see Appendix B.

We consider a streetcar moving on a graduated rectilinear axis. The initial position-velocity pair of the streetcar is assume to be $(0, 0)^T$, we call respectively $x(t)$ and $y(t)$ the position and velocity of the streetcar at time t. The objective is to steer the system from $(0, 0)^T$ to $y_f \in \mathbb{R}^2$ in minimal time. The control system reads

$$\begin{cases} \dot{y}_1(t) = y_2(t), \quad t > 0 \\ \dot{y}_2(t) = u(t), \end{cases} \tag{15}$$

which corresponds to the matrices

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{16}$$

For a fixed $M > 0$, the chosen constraint is given by

$$\mathcal{U} = \{u \in \mathbb{R}, \ |u| \leq M\}.$$

Resolution method. First, we compute the support function

$$\forall u \in \mathbb{R}, \quad \sigma_{\mathcal{U}}(u) = M|u|,$$

which is a particular case of (5).

Here, we use the functional $J_{\mathrm{d},1}$ and the estimate given by Corollary 9. Given how simple $\sigma_{\mathcal{U}}$ and the controlled system are, we acknowledge that one could actually compute the functional J itself and only have to deal with round-off errors. We do not pursue this approach since we aim at analysing how prominent the discretisation errors may be.

The Jordan-Chevalley decomposition of A is straightforward in this case, since the matrix A is itself nilpotent, of index $\ell = 2$. In this case, we hence have $\mu = 0$, $\kappa(P) = 1$, $\ell = 2$, $Q_2(x) = 1 + x$, leading to the estimate

$$|J(p_f) - J_{\mathrm{d},1}(p_f)| \leq \frac{1}{2} \Delta t \ MT \|B\| \|A^* p_f\| Q_2(\|A\|T).$$

Results. To highlight the dependence of J with respect to the target y_f, we will temporarily rename $J(p_f)$ to $J(p_f; y_f)$. We give examples of targets $y_f \in \mathbb{R}^2$ that are certified to not be $\mathcal{U}$-reachable below, in the form of a computer-assisted theorem.

Theorem 15. *The following targets are not $\mathcal{U}$-reachable from* $(0,0)$ *in time* $T = 1$*, with* $M = 1$

$$y_1 = (0.1, 0.6)^T, \qquad y_2 = (0.5, 1.1)^T, \qquad y_3 = (0.3, 0)^T.$$

Indeed, the dual certificates

$$p_1 = (-0.77, 0.64)^T, \qquad p_2 = (0.29, 0.96)^T, \qquad p_3 = (0.85, -0.53)^T.$$

provide the intervals

$$J(p_1; y_1) \in [-0.0305, -0.0291] \quad J(p_2; y_2) \in [-0.0964, -0.0959], \quad J(p_3; y_3) \in [-0.0282, -0.0268].$$

The targets and dual certificates are plotted in Figure 2, along with the theoretically known reachable set.

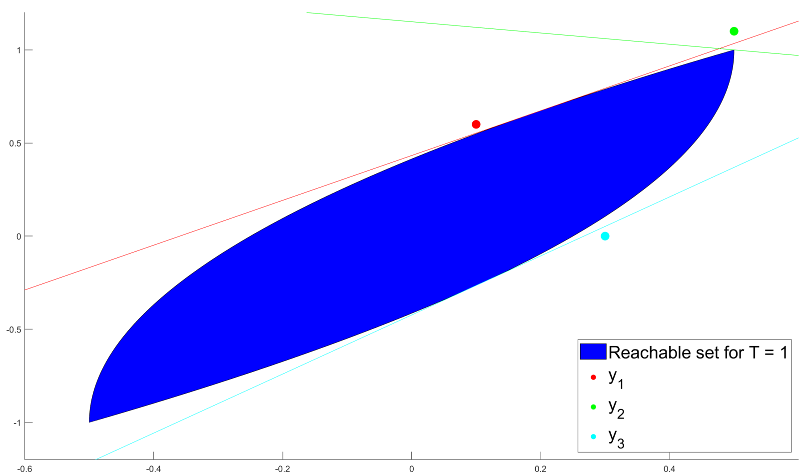

Figure 2: Non-$\mathcal{U}$ reachability of various targets from $(0,0)^T$ at time $T = 1$ for $M = 1$, together with the support hyperplane associated to their respective dual certificates, for the streetcar control problem.

Using the formula provided in Appendix B, the minimal times to reach y_1, y_2 and y_3 are computed to be slightly above 1.1656, 1.7480 and 1.0954, which means they are indeed not reachable.

4.3 Space rendezvous

Control problem. We here consider the 2-dimensional linearised Hill-Clohessy-Wiltshire equations, as defined in [7]. These equations model the motion of a follower spacecraft in the neighbourhood of a reference spacecraft (at position $(0,0,0,0)$).

$$\begin{cases} \dot{y}(t) = Ay(t) + Bu(t) & \forall t \in [0,T] \\ y(0) = y_0 \in \mathbb{R}^4, \end{cases} \tag{17}$$

where

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 3 & 0 & 0 & 2 \\ 0 & 0 & -2 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{18}$$

Note that y_1, y_2 are positions and $y_3 = \dot{y}_1$, $y_4 = \dot{y}_3$ are the corresponding speeds.

We consider the following constraint set for fixed $M_2 > 0$, $M_\infty > 0$:

$$\mathcal{U} = \{u \in \mathbb{R}^2,\ \|u\|_2 \leq M_2,\ \|u\|_\infty \leq M_\infty\}, \tag{19}$$

hence we may take $M = \min(M_2, \sqrt{2}M_\infty)$.

Let us compute the support function $\sigma_{\mathcal{U}}$ in the case where $M_\infty \leq M_2 \leq \sqrt{2}M_\infty$, that we will consider hereafter. As illustrated in Figure 3, the constraint set is the intersection of a disk and a square. Observe that the boundary of $\mathcal{U}$ is the union of flat and circular parts, whose coordinates (x, y) of intersection points form the set

$$\mathcal{P} = \left\{\left(\pm M_\infty, \pm\sqrt{M_2^2 - M_\infty^2}\right)\right\} \bigcup \left\{\left(\pm\sqrt{M_2^2 - M_\infty^2}, \pm M_\infty\right)\right\}.$$

Let us write $\partial\mathcal{U} = \mathcal{F} \cup \mathcal{C}$, where $\mathcal{F}$ (resp. $\mathcal{C}$) denotes the union of all flat (resp. circular) parts of the boundary.

Let us fix $x \in \mathbb{R}^2$. We distinguish between two cases:

- if $(O; x) \cap \partial\mathcal{U} \subset \mathcal{C}$, meaning that $\frac{\|x\|_\infty}{M_\infty} \leq \frac{\|x\|_2}{M_2}$, then $M_2\frac{x}{\|x\|_2} \in \mathcal{U}$ and using the Cauchy-Schwarz inequality, we get

$$\sigma_{\mathcal{U}}(x) \leq \sup_{y \in \mathcal{U}} \|x\|_2\|y\|_2 = \left\langle x, M_2\frac{x}{\|x\|_2}\right\rangle = M_2\|x\|_2.$$

  We thus infer that $\sigma_{\mathcal{U}}(x) = M_2\|x\|_2$.

- Otherwise, $\sigma_{\mathcal{U}}(x)$ reads as the maximum of a linear (convex) function on a union of flat parts. We easily infer that $\sigma_{\mathcal{U}}(x) = \langle p_x, x\rangle$, where p_x denotes any point of the set $\operatorname{argmin}_{p \in \mathcal{P}} \|p - x\|_2$.

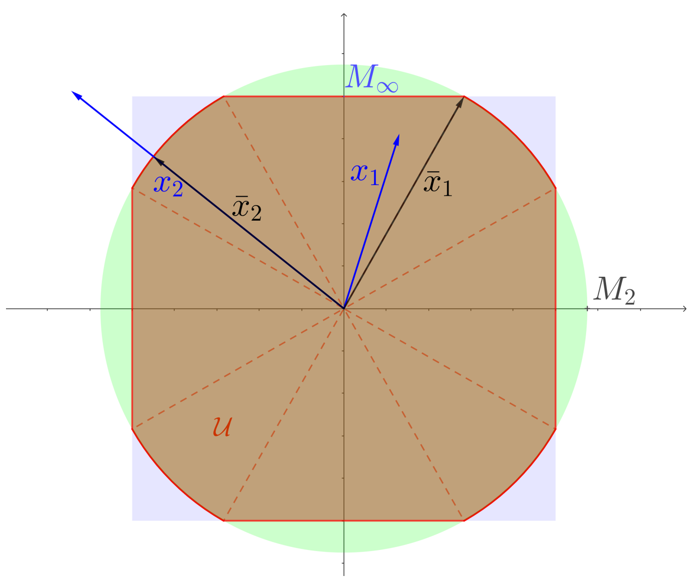

Figure 3: Construction of the support function for the rendezvous problem. One has in particular $\sigma_{\mathcal{U}}(x_i) = \langle x_i, \bar{x}_i\rangle$, $i = 1, 2$.

Resolution method. The Jordan-Chevalley decomposition of A is given by $A = D + N$ with

$$D = P\begin{pmatrix}0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & -i & 0\\ 0 & 0 & 0 & i\end{pmatrix}P^{-1}, \quad N = P\begin{pmatrix}0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}P^{-1}, \quad P = \begin{pmatrix}0 & -\frac{2}{3} & -1 & -1\\ 1 & 0 & 2i & -2i\\ 0 & 0 & i & -i\\ 0 & 1 & 2 & 2\end{pmatrix}.$$

Here, we also use the functional $J_{\mathrm{d},1}$ and the estimate given by Corollary 9. Using the corresponding notations, we have $\mu = 0$, and the index of the nilpotent matrix N is $\ell = 2$. Thus the corresponding estimate reads

$$|J(p_f) - J_{\mathrm{d},1}(p_f)| \leq \frac{1}{2}\Delta t\ MT\|B\|\|A^*p_f\|\kappa(P)Q_2(\|N\|T),$$

with $Q_2(x) = 1 + x$.

Results. Given a target $y_f \in \mathbb{R}^4$, we can derive a lower-bound on the minimal time needed to steer the system from $y_0 = (0,0,0,0)^T$ to y_f. Proposition 7 ensures that we may indeed estimate the corresponding minimal time from below, using our approach. To compute this lower bound, we apply a bisection algorithm over the set of positive real numbers, starting from a predefined interval $[t_{\mathrm{inf}}, t_{\mathrm{sup}}]$, and expanding it by multiplying its length by 2 until we cannot prove the non-reachability in time t_{sup}, and we can prove it in time t_{inf}. Then, the standard bisection method applies until the interval is reduced to the desired length.

First, we consider the time-minimal control problem of steering the system from $y_0 = (0,0,0,0)^T$ to some other position at 0 speed, i.e., $y_f = (y_1, y_2, 0, 0)^T$ for various values of $(y_1, y_2) \in \mathbb{R}^2$. Since the control problem is linear and the constraints centrally symmetric (i.e., $\mathcal{U} = -\mathcal{U}$), if y_f is reachable in time $T > 0$, so is $-y_f$. This translates into the identity $J(p_f; y_f) = J(-p_f; -y_f)$, allowing us to focus our computations on the right half-plane.

Using the bounds $M_2 = 1.15$ and $M_\infty = 1$, we obtain the certified lower bounds on the minimal-time shown on Figure 4(a). For conciseness, we do not provide the corresponding dual certificates. For comparison purposes, the minimum times computed using the Python package Gekko [4] are presented in Figure 4(b). Note that Gekko does not control discretisation bounds nor roundoff errors, hence the corresponding estimates are by no means certified.

Computation times. As is common, our certified method comes at the price of increased computation times: each step of the bisection algorithm is rather fast (about 30 seconds), but depending on parameters and how good the initial guess is, the number of iterations of the bisection algorithm may go from 3-4 to 10-15 iterations, whereas Gekko's method computes one approximation of the minimal time in about 10 seconds.

Assuming that Gekko produces reliable estimates, the accuracy of our method seems to decrease the further the target y_f is from y_0, going from about 1.8% to 37%. This can be explained as follows: our computations were made with a fixed number of time steps, namely $N_t = 20,000$; hence the higher the theoretical minimal time is, the harder it is to establish a tight lower-bound. Increasing N_t allows for a more precise approximation: for example, for $y_f = (0.5, 0.5, 0, 0)^T$, with $N_t = 400,000$, the dual certificate $p_f = (0.874, 0.0914, -0.3008, 0.3704)^T$ proves the bound $t_{\min} \geq 3.4$, which is about 3.7% away from Gekko's approximation.

On the other hand, Gekko seems to produce what might be artefacts (points $(0.1, -0.4)^T$ and $(0.2, -0.5)^T$), while our computed certified lower bounds remain smooth.

More complex unsafe set $\mathcal{Y}_f$. Now we look at the case where ones wants to avoid a given spherical object *in space*, motionless in the considered referential, regardless of the speed. In other words, for a fixed choice of $(z_1, z_2) \in \mathbb{R}^2$, and $\varepsilon > 0$, we consider

$$\mathcal{Y}_f = \left\{(y_1, y_2, y_3, y_4) \in \mathbb{R}^4,\ \|(y_1 - z_1, y_2 - z_2)\|_{\mathbb{R}^2} \leq \varepsilon\right\}, \tag{20}$$

In that case, letting $z := (z_1, z_2, 0, 0)$, the support function of $\mathcal{Y}_f$ can be computed to be

$$\sigma_{\mathcal{Y}_f} : x \longmapsto \langle z, x\rangle + \varepsilon\|z\|_2 + \delta_{\{x\in\mathbb{R}^4,\ x_3 = x_4 = 0\}}.$$

We prove below a certified result for one such example.

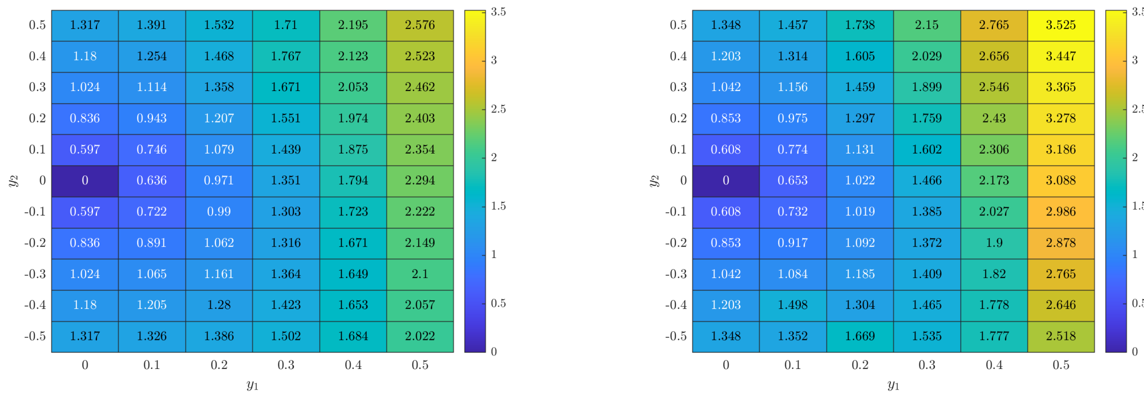

Figure 4: Estimates of the minimal time for reachability of various targets at speed 0 for the spacecraft rendezvous control problem. Certified lower bounds (left panel (a)) versus minimal times outputted by Gekko Optimization Suite [4] (right panel (b)).

Theorem 16. *Take $z_1 = z_2 = 0.5$, $\varepsilon = 0.1$, $M_2 = 1.15$, $M_\infty = 1$ and $T = 1$. Then $\mathcal{Y}_f$ is not $\mathcal{U}$-reachable from $(0,0,0,0)^T$ in time T. Indeed, we find*

$$J(p_f) \in [-0.1146, -0.0717], \quad \textit{with} \quad p_f = (0.62, 0.78, 0, 0)^T.$$

4.4 Negative semi-definite Jacobi matrices

Control problem. In this section, we report on results for some randomly generated Jacobi matrices, with varying state dimensions n. That is, we consider matrices of the form

$$A = \begin{pmatrix} a_1 & c_1 & 0 & \dots & 0 \\ c_1 & a_2 & c_2 & \ddots & \vdots \\ 0 & c_2 & a_3 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & c_{n-1} \\ 0 & \dots & 0 & c_{n-1} & a_n \end{pmatrix}. \tag{21}$$

with $a = (a_1, \dots, a_n) \in \mathbb{R}^n$, $c = (c_1, \dots, c_{n-1}) \in \mathbb{R}^{n-1}$.

These matrices are real symmetric, and up to our knowledge, no closed-form expressions are known for their eigenvalues and eigenfunctions, except in the specific case where the c_i's are all equal. Hence, for large values of n, diagonalising A becomes intractable. Even if it were accessible, it would be prone to numerical errors and we are not aware of any software that does produce such a diagonalisation within interval arithmetic.

We generate such a matrix in the following way: let $K > 0$ and $L > 0$. We draw the c_i's uniformly in $[-K, K]$. Then, we draw the a_i's uniformly in $(-2K - L, -2K]$. Thanks to the Gershgorin circle theorem, the resulting matrix is negative semi-definite.

Remark 17. *For the Jacobi matrices under consideration, the necessary and sufficient condition in Gershgorin circle theorem writes:*

$$\begin{aligned} &a_1 \le -|c_1|, \quad a_n \le -|c_{n-1}| \\ &a_i \le -|c_{i-1}| - |c_i|, \quad \forall i \in \{2, \dots, n-1\}. \end{aligned} \tag{22}$$

One could hence draw the c_i's and then draw each a_i in $(-|c_{i-1}| - |c_i| - L', -|c_{i-1}| - |c_i| - 1]$. This would allow for a broader class of Jacobi matrices, but would require additional interval arithmetic in order to guarantee condition (22).

We consider a single control u, thus $m = 1$. The corresponding matrix $B \in \mathbb{R}^{n\times 1}$ is $B = (1, \dots, 1)^T$. For a fixed $M > 0$, the constraint set is given by

$$\mathcal{U} = \{u \in \mathbb{R},\ |u| \leq M\},$$

for which we have $\sigma_{\mathcal{U}}(u) = M|u|$. The target y_f is chosen randomly, with i.i.d entries uniformly in $[0, 1]$, then renormalised such that $\|y_f\| = 0.1$.

Resolution method. Under the assumption (22), all eigenvalues of A are nonpositive according to the Gershgorin circle theorem.

As a result, we are dealing with negative semi-definite matrices, enabling us to use estimates coming from Proposition 13 upon using the Euler implicit scheme to approximate the matrix exponential.

Results. In the following example, we shall take $M = 1$, $T = 1$, $N_t = 1{,}000$ and $y_0 = 0$.

For each chosen dimension n, we generate 10 experiments with a target y_f and a random matrix A drawn as explained previously (with $K = 2$, $L = 0.1$), running our descent algorithm to try and prove the non-reachability of y_f from y_0. The following table shows the resulting means, for the midpoint and size of the obtained intervals $J(p_f)$, where p_f is the last iterate of the descent algorithm.

n	mean of the midpoints	mean of the radii
2	-0.7096	0.1166
5	-0.6233	0.1425
10	-0.5662	0.1929
20	-0.6696	0.2900
50	-0.6752	0.4739
100	-0.5873	0.6564

As can be seen, although the midpoints of intervals are rather constant, the error term steadily increases, which leads to more difficult proofs of non-reachability.

This can be circumvented by increasing the number of time steps N_t, which leads to a reduction of the error term at the expense of increased computation time.

Acknowledgements. All four authors acknowledge the support of the ANR project TRECOS, grant number ANR-20-CE40-0009. We warmly thank Fondation des Treilles, where part of this work has been conducted.

We are also grateful to Siegfried Rump for his answers regarding INTLAB.

A Convex analytic interpretation

Here, we make the additional assumption that the constraint set $\mathcal{U}$ is not only compact, but also convex. For all the following definitions and results, we refer e.g. to [3].

We let H be a Hilbert space. We recall that a function $f : H \to \mathbb{R} \cup \{+\infty\}$ is said to be *proper* if it is not identically equal to $+\infty$.

Definition-Proposition 18. *We define*

$$\Gamma_0(H) = \{f : H \to \mathbb{R} \cup \{+\infty\},\ f \text{ convex, lower semi-continuous and proper}\}.$$

We denote by $f^* : H \to \mathbb{R} \cup \{+\infty\}$ *the convex conjugate of* $f \in \Gamma_0(H)$

$$f^* : y \mapsto \sup_{x\in H} \langle x, y\rangle - f(x).$$

Furthermore, f^* *belongs to* $\Gamma_0(H)$.

Definition 19. *For $C \subset H$ a nonempty closed convex subset, we denote by $\delta_C : H \to \mathbb{R} \cup \{+\infty\}$ the convex indicator function of C*

$$\delta_C : x \mapsto \begin{cases} 0 & \text{if } x \in C \\ +\infty & \text{if } x \notin C. \end{cases}$$

We have $\delta_C \in \Gamma_0(H)$.

By definition, note that $\delta_C^* = \sigma_C$.

Theorem 20 (Weak and strong duality)**.** *Let E, X be two Hilbert spaces, $K \in L(E, X)$, $F \in \Gamma_0(E)$, and $G \in \Gamma_0(X)$. Then we have the following so-called weak duality*

$$\inf_{x \in E} F(x) + G(Kx) \geq - \inf_{y \in X} F^*(K^* y) + G^*(-y).$$

If in addition there exists $p_f \in X$ such that F^* is continuous at $L_T^* p_f$, then strong duality holds, i.e.,

$$\inf_{x \in E} F(x) + G(Kx) = - \inf_{y \in X} F^*(K^* y) + G^*(-y).$$

Fenchel-Rockafellar interpretation of our approach. Since the compact constraint set $\mathcal{U}$ is assumed to be convex, so is the set

$$\mathcal{U}_T = \{u \in E,\, t \in (0, T),\ u(t) \in \mathcal{U} \text{ for a.e. } t \in (0, T)\}.$$

An alternative approach to the one leading to Proposition 2 is then to remark that $\mathcal{Y}_f$ is $\mathcal{U}$-reachable from y_0 in time T if and only if

$$\exists u \in E, \quad \delta_{\mathcal{U}_T}(u) + \delta_{\mathcal{Y}_f - e^{TA} y_0}(L_T u) = 0,$$

in other words if and only if

$$\inf_{u \in E} \delta_{\mathcal{U}_T}(u) + \delta_{\mathcal{Y}_f - e^{TA} y_0}(L_T u) = 0.$$

Note that the above functional takes at most two values, 0 and $+\infty$. Denoting

$$F := \delta_{\mathcal{U}_T}, \qquad G := \delta_{\mathcal{Y}_f - e^{TA} y_0}, \tag{23}$$

we have $F \in \Gamma_0(E)$, $G \in \Gamma_0(\mathbb{R}^n)$ and we find that

$$F^*(L_T^* p_f) + G^*(-p_f) = \sigma_{\mathcal{U}_T}(L_T^* p_f) - \sigma_{\mathcal{Y}_f - e^{TA} y_0}(-p_f) = J(p_f).$$

Furthermore, it is easily seen that F^* is continuous at $0 = L_T^* 0$. Thus we can apply Proposition 20 to obtain the strong duality

$$\inf_{u \in E} \delta_{\mathcal{U}_T}(u) + \delta_{\mathcal{Y}_f - e^{TA} y_0}(L_T u) = - \inf_{p_f \in \mathbb{R}^n} J(p_f).$$

In particular, we see that if there exists p_f such that $J(p_f) < 0$, then $\inf_{p_f \in \mathbb{R}^n} J(p_f) < 0$ (in which case this infimum even equals $-\infty$), hence the infimum on the left-hand side equals $+\infty$, and $\mathcal{Y}_f$ is not $\mathcal{U}$-reachable from y_0 in time T. Conversely, if $\mathcal{Y}_f$ is not $\mathcal{U}$-reachable from y_0 in time T, the left-hand side equals $+\infty$, which leads to $\inf_{p_f \in \mathbb{R}^n} J(p_f) = -\infty$, so that there exists $p_f \in \mathbb{R}^n$ satisfying $J(p_f) < 0$.

B Minimal time for the streetcar example

Proposition 21. *Let* $(x_f, y_f) \in \mathbb{R}^2$*. The minimal time to steer System* (15) *from* $(0,0)$ *to* (x_f, y_f) *reads*

$$T = \frac{-sy_f + 2\sqrt{\frac{1}{2}y_f^2 + sMx_f}}{M}, \quad \text{with } s = \operatorname{sign} f(x_f, y_f),$$

using the convention $\operatorname{sign}(0) = 0$*, where* $f : \mathbb{R}^2 \to \mathbb{R}$ *is given by*

$$f(x,y) = x - \frac{1}{2M} y^2 \operatorname{sign}(y).$$

Proof. Let T be the optimal time steering System (15) from $(0,0)$ to (x_f, y_f). According to [20, Chapter 1], it is well-known that optimal controls are bang-bang equal a.e. to M or $-M$, with at most one switch, on the so-called switching locus defined by the implicit equation $f(x,y) = 0$.

More precisely, if $s < 0$, then the optimal control $u = M\mathbb{1}_{(0,t_0)} - M\mathbb{1}_{(t_0,T)}$, where $t_0 \geq 0$ is the switching time, in other words the first time such that $f(x(t), y(t)) = 0$. Conversely, if $s > 0$, then $u = -M\mathbb{1}_{(0,t_0)} + M\mathbb{1}_{(t_0,T)}$. Easy but lengthy computations yield

- If $f(x_f, y_f) = 0$, then for every $t \in [0,T]$, one has

$$y(t) = y_0 - Mt \operatorname{sign}(y_f) \quad \text{and} \quad x(t) = x_f - y_f t - \frac{1}{2}Mt^2 \operatorname{sign}(y_f).$$

- Conversely, if $f(x_f, y_f) \neq 0$, then for every $t \in [0,T]$, one has

$$\begin{aligned} y(t) &= (-y_f - sMt)\mathbb{1}_{(0,t_0)} + (y_f + sM(t - 2t_0))\mathbb{1}_{(t_0,T)} \\ x(t) &= \left(x_f - y_f t - \tfrac{1}{2}sMt^2\right)\mathbb{1}_{(0,t_0)} + \left(x_f - y_f t + sM(\tfrac{1}{2}t^2 - 2t_0 t + t_0^2)\right)\mathbb{1}_{(t_0,T)}. \end{aligned}$$

To conclude, it is important to notice that if $s \neq 0$, then $\operatorname{sign}(y(t_0)) = s$, which can be easily seen by distinguishing between several cases, depending on the sign of y_f and s.

To conclude, it remains to compute the switching time t_0. We claim that if $f(x_0, y_0) \neq 0$, then

$$t_0 = \frac{1}{M}\left(-s\, y_f + \sqrt{\frac{1}{2}y_f^2 + s\, Mx_f}\right).$$

Indeed, t_0 is characterised by the equation $f(x(t_0), y(t_0)) = 0$, which rewrites as the second order polynomial equation in the variable t_0:

$$0 = \left(x_f - s\,\frac{1}{2M}y_f^2\right) - y_f(1 + s^2)t_0 - s\, Mt_0^2.$$

Furthermore, the discriminant of this polynomial is positive. It follows that $y(T) = -y_f + sM(T - 2t_0)$ and therefore, $T = \frac{s}{M}y_f + 2t_0$. The expected conclusion follows. □

References

[1] M. Althoff, G. Frehse, and A. Girard. Set propagation techniques for reachability analysis. *Annual Review of Control, Robotics, and Autonomous Systems*, 4:369–395, 2021.

[2] R. Baier, C. Büskens, I. A. Chahma, and M. Gerdts. Approximation of reachable sets by direct solution methods for optimal control problems. *Optimization Methods and Software*, 22(3):433–452, 2007.

[3] H. Bauschke and P. Combettes. Convex analysis and monotone operator theory in hilbert spaces. *CMS books in mathematics). DOI*, 10:978–1, 2011.

[4] L. D. R. Beal, D. C. Hill, R. A. Martin, and J. D. Hedengren. Gekko optimization suite. *Processes*, 6(8), 2018.

[5] R. F. Brammer. Controllability in linear autonomous systems with positive controllers. *SIAM Journal on Control*, 10(2):339–353, 1972.

[6] A. Chambolle and T. Pock. A first-order primal-dual algorithm for convex problems with applications to imaging. *Journal of mathematical imaging and vision*, 40(1):120–145, 2011.

[7] D. Chen and K. Fudjimoto. Rendezvous control of spacecraft via constrained optimal control using generating functions. *Transactions of the japan society for aeronautical and space sciences, aerospace technology Japan*, 16(5):392–397, 2018.

[8] M. Chen and C. J. Tomlin. Hamilton–jacobi reachability: Some recent theoretical advances and applications in unmanned airspace management. *Annual Review of Control, Robotics, and Autonomous Systems*, 1(1):333–358, 2018.

[9] J.-M. Coron. *Control and nonlinearity*, volume 136 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2007.

[10] S. Ervedoza. Control issues and linear projection constraints on the control and on the controlled trajectory. *North-West. Eur. J. Math.*, 6:165–197, 2020.

[11] M. Fashoro, O. Hajek, and K. Loparo. Controllability properties of constrained linear systems. *Journal of optimization theory and applications*, 73:329–346, 1992.

[12] A. Girard, C. Le Guernic, and O. Maler. Efficient computation of reachable sets of linear time-invariant systems with inputs. In *Hybrid Systems: Computation and Control: 9th International Workshop, HSCC 2006, Santa Barbara, CA, USA, March 29-31, 2006. Proceedings 9*, pages 257–271. Springer, 2006.

[13] N. J. Higham. *Functions of matrices: theory and computation*. SIAM, 2008.

[14] J. Klamka. Constrained controllability of nonlinear systems. *Journal of Mathematical Analysis and Applications*, 201(2):365–374, 1996.

[15] H. Kong, E. Bartocci, and T. A. Henzinger. Reachable set over-approximation for nonlinear systems using piecewise barrier tubes. In H. Chockler and G. Weissenbacher, editors, *Computer Aided Verification*, pages 449–467, Cham, 2018. Springer International Publishing.

[16] A. B. Kurzhanski and P. Varaiya. On ellipsoidal techniques for reachability analysis. part i: external approximations. *Optimization methods and software*, 17(2):177–206, 2002.

[17] A. B. Kurzhanski and P. Varaiya. On ellipsoidal techniques for reachability analysis. part ii: Internal approximations box-valued constraints. *Optimization methods and software*, 17(2):207–237, 2002.

[18] C. Le Guernic and A. Girard. Reachability analysis of hybrid systems using support functions. In A. Bouajjani and O. Maler, editors, *Computer Aided Verification*, pages 540–554, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[19] C. Le Guernic and A. Girard. Reachability analysis of linear systems using support functions. *Nonlinear Analysis: Hybrid Systems*, 4(2):250–262, May 2010. Special Issue: IFAC World Congress 2008.

[20] E. B. Lee and L. Markus. *Foundations of optimal control theory*. Robert E. Krieger Publishing Co., Inc., Melbourne, FL, second edition, 1986.

[21] J. Lions. Remarks on approximate controllability. *Journal d'Analyse Mathématique*, 59(1):103, 1992.

[22] P. Lissy and C. Moreau. State-constrained controllability of linear reaction-diffusion systems. *ESAIM: Control, Optimisation and Calculus of Variations*, 27:70, 2021.

[23] J. Lohéac, E. Trélat, and E. Zuazua. Minimal controllability time for finite-dimensional control systems under state constraints. *Automatica*, 96:380–392, 2018.

[24] J. Lohéac, E. Trélat, and E. Zuazua. Nonnegative control of finite-dimensional linear systems. *Ann. Inst. Henri Poincaré, Anal. Non Linéaire*, 38(2):301–346, 2021.

[25] I. Mitchell, A. Bayen, and C. Tomlin. A time-dependent hamilton-jacobi formulation of reachable sets for continuous dynamic games. *IEEE Transactions on Automatic Control*, 50(7):947–957, 2005.

[26] D. Pighin and E. Zuazua. Controllability under positivity constraints of semilinear heat equations. *Mathematical Control and Related Fields*, 8(3&4):935–964, 2018.

[27] D. Pighin and E. Zuazua. Controllability under positivity constraints of multi-d wave equations. *Trends in control theory and partial differential equations*, pages 195–232, 2019.

[28] C. Pouchol, E. Trélat, and C. Zhang. Approximate control of parabolic equations with on-off shape controls by fenchel duality. *Annales de l'Institut Henri Poincaré C*, pages 1–43, 2024.

[29] S. Prajna and A. Jadbabaie. Safety verification of hybrid systems using barrier certificates. In R. Alur and G. J. Pappas, editors, *Hybrid Systems: Computation and Control*, pages 477–492, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[30] A. Quarteroni, R. Sacco, and F. Saleri. *Numerical mathematics*, volume 37. Springer Science & Business Media, 2006.

[31] J. Respondek. Controllability of dynamical systems with constraints. *Systems & Control Letters*, 54(4):293–314, 2005.

[32] R. T. Rockafellar and R. J.-B. Wets. *Variational analysis*, volume 317. Springer Science & Business Media, 2009.

[33] S. M. Rump. Intlab—interval laboratory. In *Developments in reliable computing*, pages 77–104. Springer, 1999.

[34] E. Zuazua. Switching control. *Journal of the European Mathematical Society*, 13(1):85–117, 2010.