International Journal of Control
Vol. 00, No. 00, Month 200x, 1–19

RESEARCH ARTICLE

Complexity Reduction Through a Schur-Based Decomposition for Reachability Analysis of Linear Time-Invariant Systems

Shahab Kaynama[a]* and Meeko Oishi[a]

[a]*Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC V6T 1Z4, Canada*

(*Received August 28, 2010; in revised form November 24, 2010*)

This paper presents a method for complexity reduction in reachability analysis and safety-preserving controller synthesis via Schur-based decomposition. The decomposition results in either decoupled or weakly-coupled (lower dimensional) subsystems. Reachable sets, computed independently for each subsystem, are back-projected and intersected to yield an overapproximation of the actual reachable set. Moreover, applying this technique to a class of unstable LTI systems we show that when certain eigenvalue and state-constraint conditions are satisfied, further reduction of complexity is possible. Evaluating our method for a variety of examples we demonstrate that significant reduction in the computational costs can be achieved. This technique has considerable potential utility for use in conjunction with computationally intensive reachability tools.

Keywords: reachability analysis; structure decomposition; transformation; projection

1 Introduction

Reachability analysis is key for safety verification and controller synthesis of continuous and hybrid dynamical systems, yet a major obstacle in employing reachability analysis is the "curse of dimensionality" (Asarin et al. 2006). The computational complexity of reachability techniques increases with the dimension of the continuous state space, often rendering them impractical for complex real-life applications.

Efficient reachability techniques have been developed recently. The algorithms in Girard et al. (2006) and Girard and Le Guernic (2008) are designed to deal with systems with a single input that is *existentially* quantified, while the method by Kurzhanski and Varaiya (2002) is also capable of handling systems with competing inputs. The utility of these techniques, however, is restricted to problems with constraints that can either be described by specific classes of shapes (e.g. ellipsoids and zonotopes) that are simple to represent and are convex, or in the more general case of Girard and Le Guernic (2008) and Varaiya (1998), can be arbitrarily-shaped but still meet the convexity requirement. Moreover, all these techniques construct the reachable set[1] by first quantifying the time variable, computing the reachable set for that time instant, and then taking the union of these sets over the finite time horizon.

For safety analysis, on the other hand, it is shown in Mitchell (2007) that not only is the control input required to be *universally* quantified, but also the time variable must be quantified *after* all other variables have been quantified. In addition, for many safety-critical systems the ability to synthesize *safety-preserving* controllers (control inputs that if applied, would keep the system trajectories away from a given "unsafe" target set (see Lygeros et al. 1999)), and

*Corresponding author. Email: kaynama@ece.ubc.ca

[1]We use the term "set" to imply what is sometimes referred to as a "tube" (Mitchell 2007, Kurzhanski and Varaiya 2000): the set of states traversed by the trajectories over the time horizon.

ISSN: 0020-7179 print/ISSN 1366-5820 online

DOI: 10.1080/0020717YYxxxxxxxx
http://www.informaworld.com

handling of *non-convex* constraints may be of critical importance. These features are offered almost exclusively by more computationally intensive reachability tools (e.g. Mitchell 2007) that suffer from a complexity that is exponential in the dimension of the states. In this case, the backward reachable set (or in short, reachable set) for a given "unsafe" target set is the set of initial states that can reach the target in finite time, regardless of the bounded control input applied. The complement of this set is known as the *largest controlled-invariant set* and is defined as the set of all initial states for which there exist a bounded control law that keeps the trajectories emanating from those states contained within the complement of the target set (and thus safe) over the entire time horizon. Reachability in this context is closely related to the *viability kernels* (or *discriminating kernels* in the case of competing inputs) from viability theory (Aubin 1991).

With a focus on continuous linear time-invariant (LTI) systems (and by extension, hybrid systems with LTI continuous dynamics), we aim to broaden the range of applicable reachability tools for LTI systems of higher dimensionality, to enable the use of tools that would otherwise be too computationally complex to employ (e.g., Mitchell (2007), Cardaliaguet et al. (1999), Saint-Pierre (2002), Gao et al. (2006)).

We accomplish this through transformation of the system into a coordinate space in which reachability could be performed in lower-dimensional subspaces and is guaranteed to yield an overapproximation of the actual reachable set in that space. Performing reachability in lower dimensions, we obtain significant reduction in the computational costs—albeit at the expense of overapproximation. As such, we propose the use of a Schur-based decomposition, inspired by a model reduction algorithm for systems with unstable modes (Siret et al. 1977, Mahmoud and Singh 1981).

Our method decomposes LTI systems into either completely decoupled or weakly-coupled subsystems. Reachability analysis can be performed on each resulting subsystem independently. Back projecting and intersecting each of the lower-dimensional reachable sets provides an over-approximation of the actual reachable set. A Sylvester equation (or an optimization problem) is solved in order to eliminate (or minimize) the coupling between the subsystems. Additional constraints are imposed when the control input is non-disjoint across subsystems, to prevent underapproximation of the unsafe reachable set. In addition, we also provide conditions under which a subspace reachable set remains unchanged for all time and show how this can be used in conjunction with the proposed Schur-based decomposition technique to yield an even further reduction of complexity for a class of systems.

Complexity reduction for reachability analysis has been addressed by a number of researchers. In general, methods to compute reachable sets for higher dimensional systems can be divided into three categories. First are techniques that take advantage of certain representations of sets (Shishido and Tomlin 2000, Kurzhanski and Varaiya 2000, Kurzhanskiy and Varaiya 2007, Girard et al. 2006, Kvasnica et al. 2004, Krogh and Stursberg 2003). Second are techniques that make use of model reduction and approximation (Han and Krogh 2004, Girard and Pappas 2007), hybridization (Asarin and Dang 2004), projection (Mitchell and Tomlin 2003) and structure decomposition (Stipanović et al. 2003, Yazarel and Pappas 2004, Han and Krogh 2005). Finally, third are methods that combine the approaches from the first two categories. For instance, Han and Krogh (2006) employs Krylov subspace projection combined with low-dimensional polytopes to perform reachability for very large-scale systems with affine dynamics.

In Mitchell and Tomlin (2003), a projection scheme based on Hamilton-Jacobi-Bellman-Isaacs (HJBI) PDEs is considered in which the projection of the actual reachable set is overapproximated in lower dimensional subspaces where the unmodeled dimensions are treated as disturbance. Similarly, Stipanović et al. (2003) decomposes a full-order nonlinear system to either disjoint or overlapping subsystems and solves multiple HJBI PDEs in lower dimensions. The computed reachable set for each subsystem is an overapproximation of the projection of the full-order reachable set onto the subsystem's subspace. In Han and Krogh (2005), using an ϵ-decomposition procedure, affine systems are decomposed into multiple subsystems and reach-

ability is performed on each lower-dimensional subsystem.

Our main contribution is to provide an additional method, within the framework of structure decomposition, to reduce the complexity of reachability analysis for higher dimensional LTI systems. In Section 2 we formulate the decomposition problem and provide necessary preliminaries. Section 3 presents the decomposition method for two cases: decomposition that results in a) decoupled subsystems, or in b) weakly-coupled subsystems. Further reduction of complexity for a class of unstable systems is discussed and an extension of our technique to hybrid systems is also given. Section 4 demonstrates our method on several numerical examples, in 3D, 4D, and 8D. Lastly, we provide concluding remarks in Section 5.

1.1 *Common Notation*

An $n \times n$ identity matrix is denoted by I_n. The quantifiers $\exists$ and $\forall$ are existential and universal, respectively. For brevity, $\|\cdot\|$ denotes an infinity norm. In particular, for a matrix $A = [a_{ij}] \in \mathbb{R}^{m\times n}$ this norm is an induced norm defined by $\|A\| := \sup_{\mathrm{v}\neq 0} \frac{\|A\mathrm{v}\|}{\|\mathrm{v}\|}$, $\mathrm{v} \in \mathbb{R}^n$, and can be computed as $\max_{1\leq j\leq n} \sum_{i=1}^{m} |a_{ij}|$. For a Lebesgue measurable function $x : \mathbb{R} \to \mathbb{R}^n$ defined over an interval $[t_0, t_f]$, we denote $\|x(t)\| := \|x(t)\|_{\mathcal{L}_\infty[t_0,t_f]} = \sup_{t\in[t_0,t_f]} |x(t)| < \infty$.

2 Problem Formulation and Mathematical Preliminaries

Consider the dynamical system

$$\dot{x} = f(x, u, d) \tag{1}$$

with state vector $x(t) \in \mathbb{R}^n$, control input $u(t) \in \mathcal{U}$, and disturbance input $d(t) \in \mathcal{D}$, where $\mathcal{U}$ and $\mathcal{D}$ are compact subsets of $\mathbb{R}^p$ and $\mathbb{R}^q$, respectively. The vector field $f\colon \mathbb{R}^n \times \mathcal{U} \times \mathcal{D} \to \mathbb{R}^n$ is assumed to be Lipschitz in x and continuous in u and d. Denote by $\mathscr{U}_{[t_0,t_f]}$ and $\mathscr{D}_{[t_0,t_f]}$ the sets of Lebesgue measurable functions $u(\cdot)$ and $d(\cdot)$ from $[t_0, t_f]$ to $\mathcal{U}$ and $\mathcal{D}$, respectively. For every $x \in \mathbb{R}^n$, $u(\cdot) \in \mathscr{U}_{[t_0,t_f]}$, and $d(\cdot) \in \mathscr{D}_{[t_0,t_f]}$, there exists a unique trajectory $\xi_{x,t_0,u(\cdot),d(\cdot)}\colon [t_0, t_f] \to \mathbb{R}^n$ that satisfies the initial condition $\xi_{x,t_0,u(\cdot),d(\cdot)}(t_0) = x$ and the differential equation (1) almost everywhere.

Let the disturbance input assume non-anticipative strategies $\vartheta\colon \mathscr{U}_{[t_0,t_f]} \to \mathscr{D}_{[t_0,t_f]}$.[1]

Definition 2.1 (Reachable Set (Tomlin et al. 2000, 2003, Mitchell et al. 2005))**:** Given a compact target *"unsafe"* set of states $\mathcal{X}_0 \subset \mathbb{R}^n$, the backward reachable set over a finite horizon $[-\tau, 0]$, $\tau > 0$ is denoted by $\mathcal{X}_{[-\tau,0]} := \mathit{Reach}_\tau(\mathcal{X}_0) \subseteq \mathbb{R}^n$ and is the set of all initial states for which there exists a disturbance input such that the trajectories emanating from those states reach the target, regardless of the control input applied, at some time during the horizon:

$$\mathcal{X}_{[-\tau,0]} := \big\{x \in \mathbb{R}^n \mid \exists\vartheta(\cdot),\, \forall u(\cdot) \in \mathscr{U}_{[-\tau,0]},\, \exists s \in [-\tau, 0],\, \xi_{x,-\tau,u(\cdot),d(\cdot)}(s) \in \mathcal{X}_0\big\}. \tag{2}$$

Notice that, with the complement of the target set marking the *safe* region of the state space, the complement of the reachable set as defined above is the *largest controlled-invariant set*: a subset of the safe region for which there exists a control law that, if applied, renders it invariant. The Level Set Toolbox (Mitchell 2007) implementing the level-set methods (Mitchell et al. 2005) can numerically compute the reachable set (or, by duality, the largest controlled-invariant set) as well as the corresponding *safety-preserving* optimal control law.

[1] A map $\vartheta\colon \mathscr{U}_{[t_0,t_f]} \to \mathscr{D}_{[t_0,t_f]}$ is non-anticipative if for every $s \in [t_0, t_f]$ and $u(\cdot), u'(\cdot) \in \mathscr{U}_{[t_0,t_f]}$, $u(s) = u'(s)$ for a.e. $s \in [t_0, t_f]$ implies $\vartheta[u](s) = \vartheta[u'](s)$ for a.e. $s \in [t_0, t_f]$. (Evans and Souganidis 1984)

Now consider the case in which (1) is an LTI system of the form

$$\dot{x} = Ax + Bu \tag{3}$$

described by matrix notation

$$\left[\, A \middle| B \,\right] \tag{4}$$

with $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times p}$.

Problem 2.2: *Find an appropriate basis transformation for* (3) *such that in the new coordinate space the system can be decomposed into lower-dimensional (decoupled/weakly-coupled) subsystems for which reachable sets can be computed independently and thus more efficiently.*

A linear transformation of (4) using a non-singular matrix $T \in \mathbb{R}^{n\times n}$ is defined as

$$\left[\, T^{-1}AT \middle| T^{-1}B \,\right]. \tag{5}$$

Now consider the following definitions.

Definition 2.3: The LTI system that consists of two subsystems

$$\dot{x}_1 = A_1 x_1 + \Delta_c x_2 \tag{6}$$

$$\dot{x}_2 = A_2 x_2 \tag{7}$$

with $A_1 \in \mathbb{R}^{k\times k}$, $A_2 \in \mathbb{R}^{(n-k)\times(n-k)}$, $\Delta_c \in \mathbb{R}^{k\times(n-k)}$, $x_1(t) \in \mathbb{R}^k$, and $x_2(t) \in \mathbb{R}^{(n-k)}$, is said to be *unidirectionally coupled* since the trajectories of (6) are affected by those of (7), while (7) evolves independently from (6).

Definition 2.4: Let there be a non-singular transformation matrix $T \in \mathbb{R}^{n\times n}$, such that $[z_1^T, z_2^T]^T = T^{-1}[x_1^T, x_2^T]^T$, and

$$\dot{z}_1 = A_1 z_1 + \widetilde{\Delta}_c z_2 \tag{8}$$

$$\dot{z}_2 = A_2 z_2. \tag{9}$$

Then (8) and (9) are said to be *unidirectionally weakly-coupled* (in comparison to (6) and (7)) if

$$\|\widetilde{\Delta}_c\| \leq \|\Delta_c\|. \tag{10}$$

Definition 2.5: Let there be a non-singular transformation matrix $T \in \mathbb{R}^{n\times n}$ and a coordinate space $w = T^{-1}x$ in which (3) can be partitioned into N subsystems as

$$\dot{w}_i = \widetilde{A}_i w_i + \widetilde{B}_i u_i, \quad i = 1, \ldots, N. \tag{11}$$

The input $u(t) \in \mathcal{U} \subset \mathbb{R}^p$ is *disjoint* across these subsystems if

$$u_i(t) \in \mathcal{U}_i \subset \mathbb{R}^{p_i}, \quad p = \sum_{i=1}^{N} p_i \tag{12}$$

so that the partitioning of $\mathcal{U}$ is mutually exclusive and exhaustive.

Definition 2.6: A subsystem i in (11) is said to be *trivially-uncontrollable* if it possesses a null input matrix, i.e. $\widetilde{B}_i = \mathbf{0}$.

Next, consider the following two lemmas.

Lemma 2.7: *The Sylvester equation*

$$EX + XF + H = \mathbf{0}, \tag{13}$$

with $E \in \mathbb{R}^{k\times k}$, $F \in \mathbb{R}^{m\times m}$, *and* $H \in \mathbb{R}^{k\times m}$, *has a solution* $X \in \mathbb{R}^{k\times m}$ *if and only if* $\text{rank}\left[(F^T \otimes I_k) + (I_m \otimes E) \quad -\text{vec}(H)\right] = \text{rank}\left[(F^T \otimes I_k) + (I_m \otimes E)\right]$ *where* $\otimes$ *denotes the Kronecker product and* $\text{vec}(H)$ *is a vector formed by stacking the columns of* H *below one another. This solution is unique if and only if the eigenvalue sum* $\lambda_i(E)+\lambda_j(F) \neq 0$, $\forall i \in \{1, ..., k\}$, $\forall j \in \{1, ..., m\}$.

Proof cf. e.g. (Zhou et al. 1996, Lem. 2.7). □

Lemma 2.8 (Real Schur form)**:** *For any real matrix* $M \in \mathbb{R}^{n\times n}$ *there exists an orthogonal matrix* $U \in \mathbb{R}^{n\times n}$ *such that* $U^T M U = \widetilde{M}$ *is real upper quasi-triangular, and the eigenvalues of* M *are the eigenvalues of the block diagonals (each of dimension 2 or less) of* $\widetilde{M}$. *Furthermore, the matrix* U *can be chosen to order the eigenvalues arbitrarily.*

Proof cf. (Golub and Loan 1996, Thm's 7.1.3 and 7.4.1) and (Strang 1988, 5R). □

Remark 1 : There always exists a partitioning of $\widetilde{M}$ such that $\widetilde{M} = \begin{bmatrix} \widetilde{M}_{11} & \widetilde{M}_{12} \\ \mathbf{0} & \widetilde{M}_{22} \end{bmatrix}$. The size of the partitions can be chosen as desired, so long as each block diagonal entry (maximum size 2×2) of $\widetilde{M}$ is completely covered by exactly one of the blocks on the diagonal of the partitioned matrix.

Finally, a linear transformation of a set $\mathcal{X} \subseteq \mathbb{R}^n$ using an invertible transformation matrix $T \in \mathbb{R}^{n\times n}$ is $\mathcal{V} := \{v \in \mathbb{R}^n \,|\, v = T^{-1}x,\, x \in \mathcal{X}\}$, written with an abuse of notation as $\mathcal{V} = T^{-1}\mathcal{X}$.

3 Methodology

The outline of the approach is as follows: Via Lemma 2.8, as in Safonov and Chiang (1989), we obtain an upper block triangular A-matrix for (4). We then perform a second similarity transformation and obtain a decoupled (or weakly-coupled) block diagonal matrix by solving a Sylvester equation (or an optimization problem). Therefore, we effectively decompose the system into two either completely decoupled or unidirectionally weakly-coupled subsystems. In the case where the decomposition is decoupled, the reachable set is computed separately for each isolated subsystem. When the decomposed subsystems are unidirectionally weakly-coupled, the reachable set is computed independently for the isolated subsystem, whereas for the remaining subsystem, the effect of coupling is accounted for by treating the coupling terms as disturbance and performing reachability with competing inputs. For both decoupled and unidirectionally weakly-coupled decompositions, the intersection of back projections of the lower dimensional reachable sets is an overapproximation of the actual reachable set in the transformed coordinate space. When the control input across the decomposed subsystems is non-disjoint, a constrained optimization problem is solved in order to make one of the subsystems trivially-uncontrollable.

In the following analysis, we assume a partitioning of (4) that results in exactly two subsystems. However, the proposed method is generalizable to N subsystems by applying the same decomposition algorithm to each subsystem iteratively. A higher number of subsystems (i.e. iterated decomposition) may result in a more conservative overapproximation of the actual reachable set.

For $k < n$, we now apply Lemma 2.8 with transformation matrix $U \in \mathbb{R}^{n\times n}$ to (4) to obtain

$$\left[\begin{array}{cc|c} \widetilde{A}_{11} & \widetilde{A}_{12} & \widetilde{B}_1 \\ \mathbf{0} & \widetilde{A}_{22} & \widetilde{B}_2 \end{array}\right] \tag{14}$$

with $\widetilde{A}_{11} \in \mathbb{R}^{k\times k}$, $\widetilde{A}_{12} \in \mathbb{R}^{k\times(n-k)}$, $\widetilde{A}_{22} \in \mathbb{R}^{(n-k)\times(n-k)}$, $\widetilde{B}_1 \in \mathbb{R}^{k\times p}$, and $\widetilde{B}_2 \in \mathbb{R}^{(n-k)\times p}$.

3.1 *Disjoint Control Input*

Consider the case in which the control input is disjoint across candidate subsystems.

Proposition 3.1: *If there exists a solution $X \in \mathbb{R}^{k\times(n-k)}$ to the Sylvester equation*

$$\widetilde{A}_{11}X - X\widetilde{A}_{22} + \widetilde{A}_{12} = \mathbf{0} \tag{15}$$

then a transformation

$$W = \begin{bmatrix} I_k & X \\ \mathbf{0} & I_{(n-k)} \end{bmatrix} \in \mathbb{R}^{n\times n} \tag{16}$$

makes (14) *completely decoupled.*

Proof cf. Siret et al. (1977), Mahmoud and Singh (1981), Safonov and Chiang (1989). Applying the transformation W to (14), we obtain

$$\left[\begin{array}{cc|c} \widetilde{A}_{11} & \widetilde{A}_{11}X - X\widetilde{A}_{22} + \widetilde{A}_{12} & \widehat{B}_1 \\ \mathbf{0} & \widetilde{A}_{22} & \widehat{B}_2 \end{array}\right] = \left[\begin{array}{cc|c} \widetilde{A}_{11} & \mathbf{0} & \widehat{B}_1 \\ \mathbf{0} & \widetilde{A}_{22} & \widehat{B}_2 \end{array}\right]. \tag{17}$$

□

Notice that the resulting subsystems $\left[\,\widetilde{A}_{11}\middle|\widehat{B}_1\,\right]$ and $\left[\,\widetilde{A}_{22}\middle|\widehat{B}_2\,\right]$ have been effectively decoupled through the coordinate transformation $z = T^{-1}x$, $T = UW$. Reachability analysis (in this transformed coordinate space) can then be performed on each lower-dimensional subsystem separately.

Now consider the case in which there is no solution to the Sylvester equation (15).

Proposition 3.2: *If* (15) *does not have a solution, then the transformation* (16) *with*

$$X = \underset{Q\in\mathbb{R}^{k\times(n-k)}}{\arg\min} \|\widetilde{A}_{11}Q - Q\widetilde{A}_{22} + \widetilde{A}_{12}\| \tag{18}$$

results in unidirectionally weakly-coupled subsystems w.r.t. (14)*.*

Proof Consider $A_c := \widetilde{A}_{11}X - X\widetilde{A}_{22} + \widetilde{A}_{12} \neq \mathbf{0}$ in (17). It is clear that in the transformed coordinate space characterized by $z = (UW)^{-1}x$, $z_2 \in \mathbb{R}^{(n-k)}$ evolves independently of $z_1 \in \mathbb{R}^k$ since $\dot{z}_2 = \widetilde{A}_{22}z_2 + \widehat{B}_2u_2$. However, z_1 is affected by z_2 through A_c. That is, we have $\dot{z}_1 = \widetilde{A}_{11}z_1 + \widehat{B}_1u_1 + A_cz_2$. Note that u_i, $i = 1, 2$, is the effective portion of the input vector u for the i-th subsystem. Minimization of the infinity norm of A_c, therefore, translates into minimizing (i.e. *weakening*) the worst-case unidirectional coupling of z_1 with z_2. To see this, let $X^* = \arg\min\|\widetilde{A}_{11}Q - Q\widetilde{A}_{22} + \widetilde{A}_{12}\|$. Then the hypothesis $\|\widetilde{A}_{12}\| < \|\widetilde{A}_{11}X^* - X^*\widetilde{A}_{22} + \widetilde{A}_{12}\|$ would imply that $X^* = \mathbf{0}$ can never be a solution. Since there are no constraints in (18) imposing this restriction, by contradiction we conclude that $\|\widetilde{A}_{11}X^* - X^*\widetilde{A}_{22} + \widetilde{A}_{12}\| \leq \|\widetilde{A}_{12}\|$. Therefore, according to Definition 2.4, the resulting subsystems are unidirectionally weakly-coupled. □

Remark 2: The objective function of (18) is convex and therefore a solution always exists.

Remark 3: The main rationale behind minimizing the *infinity norm* of the unidirectional coupling term (and thus, obtaining unidirectionally-weakly coupled subsystems) is that for the purpose of reachability analysis, the infinity norm of this term will be used to formulate an upper-bound on the magnitude of the disturbance to the upper subsystem. This will be discussed further in Section 3.3.

3.2 *Non-Disjoint Control Input*

Now consider a decomposition in which the control input is non-disjoint. In this case even if the dynamics of the subsystems are completely decoupled, their evolution is tightly paired through a common input. The difficulty arises, for example, when in the reachability computation a control value deemed optimal for one subsystem is in fact non-optimal for the full-order system. Blindly performing reachability for each subsystem separately may result in an underapproximation and additional measures have to be taken to ensure the overapproximation of the actual (unsafe) reachable set.

One way to remedy this issue is by ensuring that at least one of the subsystems in the transformed coordinate space is trivially-uncontrollable. It is clear that in such a case the (otherwise non-disjoint) control action does not affect the evolution of the reachable set of the trivially-uncontrollable subsystem. Therefore, an optimal control input for the subsystem with nonzero input matrix is also optimal for the full-order system.

More formally, if either the pair $(\widetilde{A}_{22}, \widehat{B}_2)$ or the pair $(\widetilde{A}_{11}, \widehat{B}_1)$ in (17) is made trivially-uncontrollable, reachability analysis can be performed as in the disjoint control input case, separately for each subsystem.

Assumption 3.3: $\mathscr{C}(\widetilde{B}_1^T) \subseteq \mathscr{C}(\widetilde{B}_2^T)$, where $\mathscr{C}(\cdot)$ is the column-space operator.

Proposition 3.4: *The transformation* (16) *with*

$$X = \underset{Q \in \mathbb{R}^{k\times(n-k)}}{\arg\min} \|\widetilde{A}_{11}Q - Q\widetilde{A}_{22} + \widetilde{A}_{12}\| \quad \text{subject to } Q\widetilde{B}_2 = \widetilde{B}_1 \tag{19}$$

results in unidirectionally coupled subsystems. Moreover, $(\widetilde{A}_{11}, \widehat{B}_1)$ *is trivially-uncontrollable.*

Proof Assumption 3.3 is the necessary and sufficient condition for solvability of the overdetermined equality constraint in (19). To see the trivial-uncontrollability of $(\widetilde{A}_{11}, \widehat{B}_1)$ consider $\widehat{B} := W^{-1}\widetilde{B}$ in (17). We have

$$\begin{bmatrix}\widehat{B}_1\\ \widehat{B}_2\end{bmatrix} := \begin{bmatrix}I_k & -X\\ \mathbf{0} & I_{(n-k)}\end{bmatrix}\begin{bmatrix}\widetilde{B}_1\\ \widetilde{B}_2\end{bmatrix} = \begin{bmatrix}\widetilde{B}_1 - X\widetilde{B}_2\\ \widetilde{B}_2\end{bmatrix}. \tag{20}$$

Constraining the optimizer in (19) to choose from the class of solutions $\left\{X \in \mathbb{R}^{k\times(n-k)} \mid X\widetilde{B}_2 = \widetilde{B}_1\right\}$ simply enforces $\widehat{B}_1 = \mathbf{0}$. □

The resulting subsystems can now be treated as in the disjoint control input case, and hence an overapproximation of the reachable set in each subspace can be computed.

3.3 *Reachability in Lower Dimensions*

In the new coordinate space $z = T^{-1}x$, $T := UW$ reachability analysis can be performed on each lower-dimensional subsystem separately:

Algorithm 1:

$\mathcal{Z}_0 \leftarrow T^{-1}\mathcal{X}_0$
for $i \leftarrow 1, 2$ **do**
  $\mathcal{Z}_0^i \leftarrow proj(\mathcal{Z}_0, i)$ ▷ project onto i-th subspace
end for
For lower subsystem:
  $\mathcal{Z}^2_{[-\tau,0]} \leftarrow Reach_\tau(\mathcal{Z}_0^2)$
For upper subsystem:

8: Treat $A_c z_2$ as disturbance ▷ $A_c := \widetilde{A}_{11}X - X\widetilde{A}_{22} + \widetilde{A}_{12}$
9: $\xi \leftarrow \sup_{z_2 \in \mathcal{Z}^2_{[-\tau,0]}} \|z_2\|$
10: Compute upper-bound $\|A_c z_2\| \leq \|A_c\|\xi$
11: $\mathcal{Z}^1_{[-\tau,0]} \overset{\text{consrv.}}{\longleftarrow} Reach_\tau(\mathcal{Z}^1_0)$
12: **return**$(\mathcal{Z}^1_{[-\tau,0]}, \mathcal{Z}^2_{[-\tau,0]})$

Note that steps 8 through 10 of Algorithm **1** may or may not be needed depending on whether the subsystems are obtained from Propositions 3.1, 3.2, or 3.4. The following scenarios describe how the input(s) are quantified to construct the subsystem reachable sets:

- S1 (Proposition 3.1 is used): For both $\mathcal{Z}^1_{[-\tau,0]}$ and $\mathcal{Z}^2_{[-\tau,0]}$, the single input is control and it is universally quantified.
- S2 (Proposition 3.2 is used): For $\mathcal{Z}^1_{[-\tau,0]}$ the control input is universally quantified while the disturbance input (unidirectional coupling) is existentially quantified. For $\mathcal{Z}^2_{[-\tau,0]}$ the single input is control and it is universally quantified.
- S3 (Proposition 3.4 is used): For $\mathcal{Z}^1_{[-\tau,0]}$ the single input is disturbance (unidirectional coupling) and it is existentially quantified. For $\mathcal{Z}^2_{[-\tau,0]}$ the single input is control and it is universally quantified.

The overapproximation of the actual reachable set of the full-order system in $\mathbb{R}^n$ can be obtained using the following lemma.

Lemma 3.5: *Let $\mathcal{Z}^i_{[-\tau,0]}$, $i = 1, 2$, be the computed lower-dimensional overapproximative reachable set of subsystem i. Then the transformation of the intersection of the back-projection of these sets onto $\mathbb{R}^n$ overapproximates the actual full-order reachable set $\mathcal{X}_{[-\tau,0]}$ of system* (4)*. That is,*

$$\overline{\mathcal{X}}_{[-\tau,0]} := T\Big((\mathcal{Z}^1_{[-\tau,0]} \times \mathbb{R}^{(n-k)}) \cap (\mathbb{R}^k \times \mathcal{Z}^2_{[-\tau,0]})\Big) \supseteq \mathcal{X}_{[-\tau,0]}. \tag{21}$$

Proof cf. Mitchell and Tomlin (2003), Stipanović et al. (2003). □

3.3.1 Formulating an Upper-Bound on the Growth of $\mathcal{Z}^1_{[-\tau,0]}$ in Scenario S3

When the subsystems are obtained via Proposition 3.4, the reachable set in the subspace of the trivially-uncontrollable subsystem is computed without the need for solving a differential game. In fact, for this subsystem the unidirectional coupling is treated as disturbance and, therefore, it is existentially quantified. Consequently, this disturbance together with the dynamics strive to enlarge the reachable (unsafe) set as much as possible. This allows us to formulate an analytic upper-bound on the overapproximation of the reachable set in this subspace in terms of system and design parameters:

Let $\mathcal{B}(0, \alpha)$ denote an infinity norm ball of radius $\alpha \in \mathbb{R}^+$ centred around the origin in $\mathbb{R}^k$. Let $z_{1,0} \in \mathcal{Z}^1_0$ and suppose $\widetilde{\mathscr{D}}_{[-\tau,0]}$ is the set of measurable functions from $[-\tau, 0]$ to $\mathcal{B}(0, \|A_c\|\xi)$. There exists an admissible input $\tilde{d}(\cdot) \in \widetilde{\mathscr{D}}_{[-\tau,0]}$ such that in positive time using time-reversed dynamics we have

$$z_1 := \exp(-\widetilde{A}_{11}\tau)z_{1,0} - \int_0^\tau \exp(-\widetilde{A}_{11}(\tau - r))\tilde{d}(r)\mathrm{d}r, \quad z_1 \in \mathcal{Z}^1_{[-\tau,0]}. \tag{22}$$

Bounding the effect of the input on the evolution of the trajectories we obtain

$$\|z_1 - \exp(-\widetilde{A}_{11}\tau)z_{1,0}\| \leq \int_0^\tau \exp(\|\widetilde{A}_{11}\|(\tau - r))\|A_c\|\xi \mathrm{d}r \tag{23}$$

$$= \frac{\exp(\|\widetilde{A}_{11}\|\tau) - 1}{\|\widetilde{A}_{11}\|}\|A_c\|\xi \tag{24}$$

$$\leq \left(\lim_{M\to\infty}\sum_{i=1}^{M}\frac{\tau^i\big(\sqrt{k}\,\overline{\sigma}(\widetilde{A}_{11})\big)^{i-1}}{i!}\right)\|A_c\|\xi =: \mu_{[-\tau,0]} \tag{25}$$

where $\overline{\sigma}(\cdot)$ is the largest singular value operator, and k is the dimension of the trivially-uncontrollable subsystem. Therefore, an upper-bound for how much $\mathcal{Z}^1_{[-\tau,0]}$ can grow in backward time can be written as

$$\mathcal{Z}^1_{[-\tau,0]} \subseteq \Big(\bigcup_{s\in[-\tau,0]}\exp(\widetilde{A}_{11}s)\mathcal{Z}^1_0\Big) \oplus \mathcal{B}(0,\mu_{[-\tau,0]}) \tag{26}$$

in which $\oplus$ denotes the Minkowski sum.[1] In particular, the choice of k, the magnitude of the unidirectional coupling $\|A_c\|$, the supremum of the reachable set in the lower subspace $\xi = \sup_{z_2\in\mathcal{Z}^2_{[-\tau,0]}}\|z_2\|$, and the largest singular value of the upper subsystem $\overline{\sigma}(\widetilde{A}_{11})$ can all affect the conservatism of the reachable set $\mathcal{Z}^1_{[-\tau,0]}$. Moreover, given k and τ, the flexibility of the Schur form in placing the eigenvalues in any order along the block-diagonals of $\widetilde{A}$ can be exploited to make this subsystem evolve with slower dynamics. Through various tests we were able to confirm that doing so could potentially prevent the excessive growth of $\mathcal{Z}^1_{[-\tau,0]}$ by influencing both $\exp(\widetilde{A}_{11}s)$ and $\mu_{[-\tau,0]}$.

3.4 *Further Reduction of Complexity in Reachability for a Class of Unstable Systems*

We now demonstrate that for a specific class of unstable LTI systems, the Schur-based decomposition can be used to further reduce the computational burden associated with reachability analysis.

Particularly, we decompose any full-order unstable system into *stable* and *anti-stable* subsystems with disjoint input across them. To do this, we employ the presented Schur-based decomposition while rearranging the order of eigenvalues such that the lower (controlled) subsystem contains only the non-negative eigenvalues and the upper (uncontrolled and possibly perturbed) subsystem contains the strictly-negative ones. As we will show in Proposition 3.6, under certain conditions, reachability analysis in the anti-stable subspace need *not* be performed since the target and the reachable sets coincide for all time.

Proposition 3.6: *Suppose that for a controlled linear system* (3) *the following conditions are satisfied.*

(i) $\mathcal{X}_0$ *is convex (but possibly arbitrarily shaped) and contains the origin in its interior;*
(ii) the A-matrix is anti-stable (analytic in the open left-half complex plane) with repeated and real eigenvalues $\lambda_1 = \cdots = \lambda_n \geq 0$*;*
(iii) the algebraic and geometric multiplicities of $\lambda_i(A)$ *are equal.*

Then, for any $\tau > 0$*,*

$$\mathcal{X}_{[t,\,0]} = \mathcal{X}_0 \quad \forall t \in [-\tau, 0]. \tag{27}$$

[1]The Minkowski sum of any two sets $\mathcal{X}$ and $\mathcal{Y}$ in $\mathbb{R}^n$ is defined as $\mathcal{X}\oplus\mathcal{Y} = \{x + y \mid x \in \mathcal{X}, y \in \mathcal{Y}\}$.

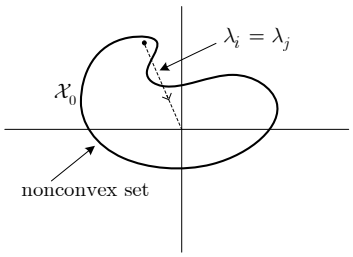


Figure 1. Phase-plane of a planar system with a nonconvex target set $\mathcal{X}_0$. Even though conditions (ii) and (iii) are satisfied, the target set $\mathcal{X}_0$ will grow in backward time.

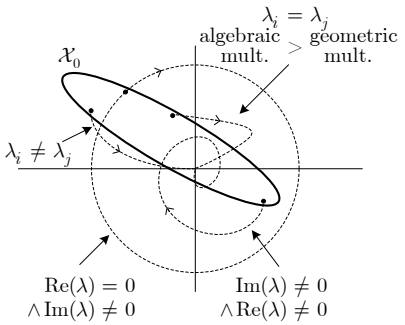


Figure 2. Phase-plane with various eigenvalue scenarios that would violate conditions of Proposition 3.6 and thus causing the target set $\mathcal{X}_0$ to grow in backward time.

Proof The proof is provided in Appendix A. □

Remark 4 : Condition (i) is easily generalizable to star-convex sets for which the origin is the convergence point (any line segment from the origin to $x \in \mathcal{X}_0$ is contained in $\mathcal{X}_0$). An example of this is when the states are constrained to l_p-space with $0 < p < 1$.

An intuitive 2-dimensional illustration of various cases that would violate conditions in Proposition 3.6 is given in Figures 1 and 2 where the trajectories are shown in backward time.

Note that although Proposition 3.6 is stated in terms of a general full-order system (and as such, may seem too restrictive), it makes the following assertion: If any isolated subsystem of any given unstable system in any coordinate space satisfies the conditions in Proposition 3.6, then the reachable set for that subsystem remains precisely equal to the target set in the respective subspace. Suppose that reachability analysis is to be performed for an unstable system $\dot{x} = Ax + Bu$, $u(t) \in \mathcal{U}$ with k negative and $(n-k)$ non-negative eigenvalues for a target set $\mathcal{X}_0$. We apply Schur-based decomposition with an appropriately synthesized transformation matrix T to obtain

$$\left[\begin{array}{cc|c} \widetilde{A}_- & A_c & \mathbf{0} \\ \mathbf{0} & \widetilde{A}_+ & \widehat{B}_2 \end{array}\right] \tag{28}$$

partitioned such that $\widetilde{A}_+$ and $\widetilde{A}_-$ contain only non-negative and strictly-negative eigenvalues, respectively. If $\widetilde{A}_+$ and $\mathcal{X}_0$ satisfy the conditions (i), (ii), and (iii), then according to Proposition 3.6 the reachable set in the lower subspace does not grow and thus need not be computed. Reachability analysis is performed only for the upper subsystem resulting in further reduction of complexity by avoiding altogether the reachable set computation in the lower subspace. Specifically, step 6 in Algorithm **1** is entirely omitted. The overapproximation of the full-order reachable set can then be calculated according to (21) with $\mathcal{Z}^1_{[-\tau,0]} = Reach_\tau(proj(T^{-1}\mathcal{X}_0, 1))$ and $\mathcal{Z}^2_{[-\tau,0]} = proj(T^{-1}\mathcal{X}_0, 2)$.

Note that linear transformation preserves convexity. Therefore the projection of the transformation of $\mathcal{X}_0$ onto the lower subspace, i.e. $\mathcal{Z}^2_0 := proj(T^{-1}\mathcal{X}_0, 2)$, is also convex if $\mathcal{X}_0$ is and contains the origin if $\mathcal{X}_0$ does.

3.5 *Extension to Hybrid Systems*

The extension of our transformation-based method to hybrid dynamical systems is fairly straight forward. Consider the hybrid automaton $(\mathfrak{Q}, \mathfrak{X}, f, \mathcal{U}, \Sigma, R)$ with discrete modes $\mathfrak{Q} = \{q_i\}$, continuous states $x \in \mathfrak{X}$, continuous control inputs $u \in \mathcal{U}$, discrete control inputs $\sigma \in \Sigma$, vector field $f : \mathfrak{Q} \times \mathfrak{X} \times \mathcal{U} \to \mathfrak{X}$, $(q_i, x, u) \mapsto A_i x + B_i u$, and transition function $R : \mathfrak{Q} \times \mathfrak{X} \times \mathcal{U} \times \Sigma \to \mathfrak{Q} \times \mathfrak{X}$.

Let $\mathcal{X}_0(q_i)$ (a set of continuous states in mode q_i) be the target set and $\mathcal{W}(q_i)$ the reachable set. Also, let T_i be the transformation matrix for mode q_i obtained from the Schur-based de-

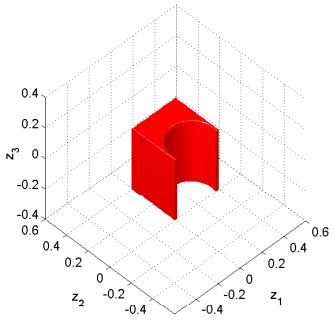


Figure 3. $\mathcal{Z}_0$: The non-convex target set in the transformed coordinate space.

composition technique described previously. As in Tomlin et al. (2003), reachability calculations proceed in each mode in parallel such that for mode q_i the reach-avoid operation becomes

$$T_i Reach_\tau\big(T_i^{-1}\mathcal{X}_0(q_i), T_i^{-1}\mathcal{W}(q_i)\big). \tag{29}$$

In case of a switched system with two modes q_i and q_j and an identity reset map, the backward reachable set $\mathcal{X}_{[-\tau,0]}$ can be directly calculated as

$$\mathcal{X}_{[-\tau,0]} = T_j Reach_\tau\Big(q_j, T_j^{-1} T_i Reach_\tau\big(q_i, T_i^{-1}\mathcal{X}_0(q_i)\big)\Big) \tag{30}$$

where T_i and T_j are the transformation matrices for modes q_i and q_j respectively. Reachability analysis is then performed on lower-dimensional subsystems in each mode according to Algorithm **1**.

4 Numerical Examples

Although complexity reduction through Schur-based decomposition can be used in conjunction with any reachability/viability technique that can accommodate both existentially and universally quantified inputs, we demonstrate the applicability and practicality of our method using a number of examples (up to 8D) that employ the Level Set Toolbox (LS) (Mitchell 2007). While LS has mainly been used for systems of low dimensionality (Bayen et al. 2007), our complexity reduction approach can facilitate the use of LS for higher dimensional systems for which safety-preserving controller synthesis and/or handling of non-convex, arbitrarily-shaped sets is important.

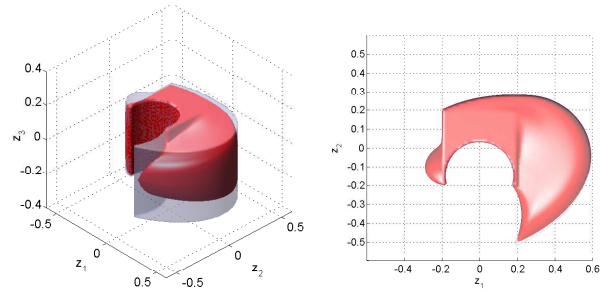
All computations are performed on a dual core Intel-based computer with 2.8 GHz CPU, 6 MB of cache and 3 GB of RAM running single-threaded 32-bit MATLAB 7.5.

4.1 *Arbitrary 3D System*

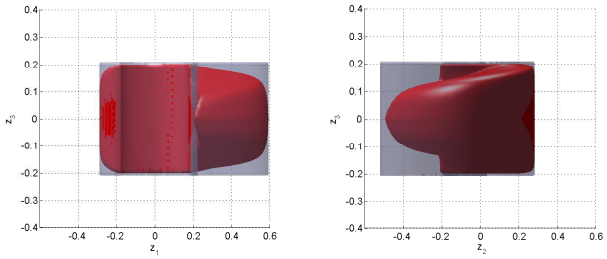
Consider an arbitrary 3D LTI system with

$$A = \begin{bmatrix} -0.5672 & -0.7588 & -0.6282 \\ 3.1364 & -1.1705 & 2.3247 \\ 1.8134 & -1.7689 & -2.6930 \end{bmatrix}, \quad B = \begin{bmatrix} 0.0731 & -0.1639 \\ -0.7377 & -0.3578 \\ 0.1470 & 0.2410 \end{bmatrix}$$

and input $u = [u_1, u_2]^T \in \mathbb{R}^2$, $\|u\| \leq 1.1$. We choose a non-convex target (unsafe) set $\mathcal{X}_0 \subset \mathbb{R}^3$ such that in the transformed coordinate space we have $\mathcal{Z}_0 = T^{-1}\mathcal{X}_0$ as shown in Figure 3. Here, T is the transformation matrix obtained through Proposition 3.1 that decomposes the system into two subsystems (one 2D and one 1D) with disjoint control across them:



(a) Comparison in z-space (b) z_1–z_2 cross-section



(c) z_1–z_3 cross-section (d) z_2–z_3 cross-section

Figure 4. Schur-based overapproximation (transparent light) vs. actual (solid dark) reachable sets in the transformed coordinate space for Example 4.1.

$$T^{-1}AT = \left[\begin{array}{cc:c} -1.6653 & -3.4560 & 0 \\ 1.8706 & -1.4653 & 0 \\ \hdashline 0 & 0 & -1.3000 \end{array}\right], \quad T^{-1}B = \left[\begin{array}{c:c} -0.7530 & 0 \\ 0.0640 & 0 \\ \hdashline 0 & 0.2500 \end{array}\right].$$

Hence, the decoupled subsystems are $\dot{z}_1 = \left[\begin{smallmatrix} -1.6653 & -3.4560 \\ 1.8706 & -1.4653 \end{smallmatrix}\right] z_1 + \left[\begin{smallmatrix} -0.7530 \\ 0.0640 \end{smallmatrix}\right] u_1$ and $\dot{z}_2 = \left[-1.3000\right] z_2 + \left[0.2500\right] u_2$.

We obtain an overapproximation of the actual reachable set, as shown in Figure 4. Reachability calculation is performed over a grid with 101 nodes in each dimension for $\tau = 2\,\mathrm{s}$. The computation time for the actual and the Schur-based reachable sets (including decomposition and projections) were 5823.73 s and 22.87 s, respectively.

4.2 *4D Aircraft Dynamics*

Consider longitudinal aircraft dynamics $\dot{x} = Ax + B\delta_e$,

$$A = \begin{bmatrix} -0.0030 & 0.0390 & 0 & -0.3220 \\ -0.0650 & -0.3190 & 7.7400 & 0 \\ 0.0200 & -0.1010 & -0.4290 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0.0100 \\ -0.1800 \\ -1.1600 \\ 0 \end{bmatrix}$$

with state $x = [u, \alpha, \dot{\theta}, \theta]^T \in \mathbb{R}^4$ comprised of deviations in aircraft speed, angle of attack, pitch-rate, and pitch angle respectively, and with input $\delta_e \in [-13.3^\circ, 13.3^\circ] \in \mathbb{R}$ the elevator deflection. These matrices represent stability derivatives of a Boeing 747 aircraft cruising at an altitude of 40 kft with speed 774 ft/sec (Bryson 1994). We define a non-convex target (unsafe) set $\mathcal{X}_0$ such that in the transformed coordinate space $\mathcal{Z}_0 = \{z \in \mathbb{R}^4 \mid \|z\| > 0.15,\ z = T^{-1}x,\ x \in \mathcal{X}_0\}$ where T is the transformation matrix obtained through our method.

We first decompose the system into two 2D subsystems. Since the control input is non-disjoint across the resulting subsystems, we use Proposition 3.4 and obtain unidirectionally coupled subsystems, one of which is trivially-uncontrollable. The reachability calculation is performed over a grid with 41 nodes in each dimension for $\tau = 5\,\mathrm{s}$. The computation time for the actual and the Schur-based reachable sets (including decomposition and projections) were 28546.80 s and 54.64 s, respectively—a significant reduction.

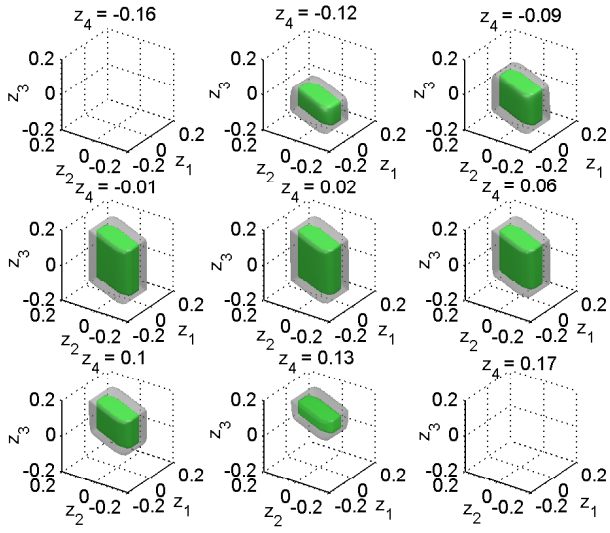


Figure 5. Schur-based (solid dark) vs. actual (transparent light) controlled-invariant sets (safe) in the transformed coordinate space for Example 4.2. The computed reachable set and its overapproximation are the non-convex complements of these objects.

Since the computed sets are 4D, we plot a series of 3D snapshots of these 4D objects at specific values of z_4 (Figure 5). The aircraft flight envelope (safe) is represented by the area inside the shaded regions.

4.3 *8D Distillation Column*

Consider the dynamic model of a binary distillation column obtained from Skogestad and Postlethwaite (2007) with

$$A = \begin{bmatrix} -0.5774 & 3.0567 & 0.0073 & -0.8121 & 0.3034 & -0.3035 & 0.0072 & -0.1542 \\ -2.7290 & -0.7147 & -0.3430 & 1.5321 & 0.6643 & 0.2896 & -0.0013 & 0.0926 \\ 0 & 0 & -0.3891 & -0.9956 & 0.0182 & 0.0235 & 0.0049 & 0.0506 \\ 0 & 0 & 1.3640 & -1.3363 & -0.9037 & -0.4686 & -0.0009 & -0.1887 \\ 0 & 0 & 0 & 0 & -0.7357 & -0.2275 & -0.0082 & -0.0021 \\ 0 & 0 & 0 & 0 & 0 & -0.2259 & 0.0021 & -0.0457 \\ 0 & 0 & 0 & 0 & 0 & 0 & -0.0052 & 0.0024 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -0.0755 \end{bmatrix}$$

$$B = \begin{bmatrix} -0.0335 & -0.4534 & -0.8005 & 0.5497 & 1.2886 & 0.3132 & 0.7117 & 0.0599 \\ -0.1228 & -0.0711 & -0.2612 & -0.1344 & -0.0504 & -0.2249 & -0.6994 & -0.3014 \end{bmatrix}^T.$$

The input $u = [u_1, u_2]^T \in \mathbb{R}^2$ with $u_1, u_2 \in [0, 1]$ is comprised of reflux and boilup flows, respectively. The full-order system with state vector $x \in \mathbb{R}^8$ is first decomposed into two (unidirectionally coupled) 4D subsystems using Proposition 3.4, since the control vector is non-disjoint across the two candidate subsystems. Similarly, each of these 4D subsystems is decomposed into two 2D subsystems. Since the upper 4D subsystem is made trivially-uncontrollable through (19), its decomposition is disjoint and therefore Proposition 3.1 is used to obtain the 1st and 2nd (decoupled) 2D subsystems. On the other hand, for the lower 4D subsystem the decomposition results in non-disjoint control input. Therefore Proposition 3.4 is employed and the 3rd and 4th (unidirectionally coupled) 2D subsystems are obtained.

Reachability is first performed on the 3rd and 4th subsystems while taking the effect of unidirectional coupling into account. Next, the reachable sets of the 1st and 2nd subsystems are computed while treating the effect of the 3rd and 4th subsystems as disturbance.

We label the 2D transformed state subspaces as $\widetilde{w}_1 = [w_1, w_2]^T$, $\widetilde{w}_2 = [w_3, w_4]^T$, $\widetilde{q}_1 = [q_1, q_2]^T$, and $\widetilde{q}_2 = [q_3, q_4]^T$. Notice that $\mathbb{R}^4 \ni q = [\widetilde{q}_1^T, \widetilde{q}_2^T]^T = T_3^{-1}\widetilde{z}_2$, $\mathbb{R}^4 \ni w = [\widetilde{w}_1^T, \widetilde{w}_2^T]^T = T_2^{-1}\widetilde{z}_1$, and $\mathbb{R}^8 \ni z = [\widetilde{z}_1^T, \widetilde{z}_2^T]^T = T_1^{-1}x$ with $\widetilde{z}_1, \widetilde{z}_2 \in \mathbb{R}^4$.

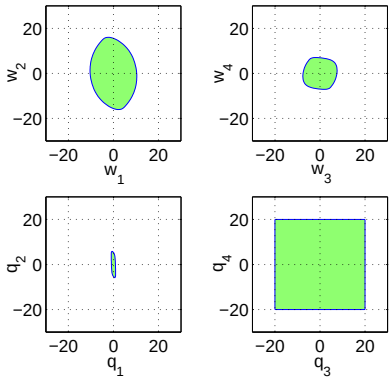


Figure 6. Safe set of Example 4.3 in transformed 2D subspaces.

We assume that the target (unsafe) set $\mathcal{X}_0 \subset \mathbb{R}^8$ is chosen such that the transformations $T_1^{-1} \in \mathbb{R}^{8\times 8}$, $T_2^{-1} \in \mathbb{R}^{4\times 4}$, and $T_3^{-1} \in \mathbb{R}^{4\times 4}$ result in $\mathcal{W}_0 := \{w \in \mathbb{R}^4 \mid \|w\| > 20\}$ and $\mathcal{Q}_0 := \{q \in \mathbb{R}^4 \mid \|q\| > 20\}$. The target sets for the 2D subsystems is simply the projection of $\mathcal{W}_0$ and $\mathcal{Q}_0$ onto their corresponding subspaces.

Lower dimensional reachability is performed over a grid with 101 nodes in each dimension for $\tau = 6$ s. The overall computation time (including decomposition and projections) was 94.31 s. The complement of the shaded regions in Figure 6 overapproximate the reachable (unsafe) set in each of the 2D subspaces. The full 8D reachable set is the intersection of the back-projection of the 2D reachable sets.

The actual reachable set is not shown since it is prohibitively computationally expensive to compute with LS.

4.4 *4D Unstable System (An Example for Section 3.4)*

Consider an unstable system (Ioannou and Sun 1996, Ex. 2.2.1) with

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0.1023 & 0 & -0.0085 & 0 \\ 0 & 0 & 0 & 1 \\ -0.0153 & \varepsilon & 0.0993 & 0 \end{bmatrix}, \quad B = 10^{-3} \times \begin{bmatrix} 0 \\ -0.8696 \\ 0 \\ 0.1304 \end{bmatrix}.$$

Let the eigenvalues of the system be slightly perturbed as determined by parameter $\varepsilon \in \mathbb{R}$. With $\varepsilon = 0.0491$ the real anti-stable eigenvalues coincide.

We apply the method described in Section 3.4 and obtain two 2D subsystems (with separated stable and anti-stable eigenvalues) across which the input is disjoint. The system matrices in the transformed coordinates are

$$T^{-1}AT = \left[\begin{array}{cc:cc} -0.3426 & 0.0354 & -0.6988 & 0.1399 \\ -0.0000 & -0.2912 & 0.9481 & -0.0000 \\ \hdashline 0 & 0 & 0.3150 & -0.0135 \\ 0 & 0 & 0.0003 & 0.3188 \end{array}\right], \quad T^{-1}B = 10^{-3} \times \left[\begin{array}{c} 0 \\ 0 \\ \hdashline -0.7621 \\ 0.3426 \end{array}\right].$$

A target (unsafe) set $\mathcal{X}_0$ is chosen such that $\mathcal{Z}_0 = \{z \in \mathbb{R}^4 \mid \sqrt{z^T z} \leq 0.2,\ z = T^{-1}x,\ x \in \mathcal{X}_0\}$, i.e. a small Euclidean ball of radius 0.2 around the origin. The magnitude of the input is bounded by $|u| \leq 1$. Using reachability analysis we attempt to identify the set of initial states that reach $\mathcal{Z}_0$ in $\tau = 3$ seconds, regardless of the input applied.

Since all conditions in Proposition 3.6 are satisfied for the lower subsystem, to obtain an over-approximation of the full-order system, we only compute the overapproximation of the reachable set in its stable subspace. The reachable set and its overapproximation are shown in Figure 7. Reachability was performed over a grid with 41 nodes in each dimension. The overall computation time (including decomposition and projections) was 2.8 s. In comparison, computing the reachable set of the full-order system would require 1741.6 s.

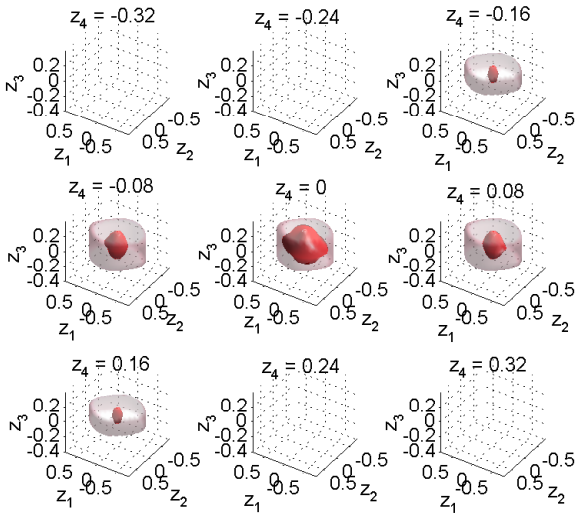


Figure 7. 3D snapshots of the actual (solid dark) unsafe reachable set vs. its overapproximation (transparent light) in the transformed coordinate space. The overapproximation was computed using Schur-based decomposition in conjunction with Proposition 3.6 for only one of the subsystems.

5 Conclusions and Future Work

We presented a Schur-based decomposition for reachability analysis of LTI systems. This decomposition has considerable potential for reducing the computational complexity in reachable set calculations, especially for reachability tools that are computationally intensive (such as the Level Set Toolbox). The decomposition was evaluated in terms of whether the resulting subsystems had disjoint or non-disjoint control inputs. In the event that a Sylvester equation can be solved, the decomposition yields two decoupled subsystems. When the Sylvester equation cannot be solved, its minimization yields two weakly coupled subsystems. A constrained optimization problem is considered for the case in which the control input is non-disjoint across decomposed subsystems. We applied this technique to a variety of examples computed with the Level Set Toolbox, and found computational time significantly reduced when our method was employed. Furthermore, we presented conditions under which the backward reachable and the target sets coincide. We then showed that the proposed Schur-based decomposition can be used together with these conditions in order to significantly reduce the computational complexity of reachability analysis for a class of unstable systems.

Future work includes efforts to reduce potential conservatism in the overapproximation of the reachable set. One direction is in a time-dependent formulation of the disturbance to the upper subsystem by performing reachability in sub-time intervals. A second direction is in an alternative transformation in the trivially-uncontrollable case, that produces subsystems that may all be controlled to some degree while still preserving the disjoint property of the input. If the target set in the new coordinate space is far from being axis-aligned, the projections contribute to the conservatism of the reachable set overapproximation. A third direction, therefore, is in incorporating the geometric information about the shape of the target set into the decomposition process so that the projection of the set onto the subspaces of the transformed coordinates does not result in excessive loss of detail.

Acknowledgment

The authors thank Ian Mitchell for valuable discussions, and the anonymous reviewers for their constructive comments. This research was supported by NSERC Discovery Grant #327387 (M. Oishi) and NSERC Collaborative Health Research Project #CHRPJ-350866-08 (G. Dumont).

References

Asarin, E., and Dang, T. (2004), "Abstraction by projection and application to multi-affine systems," in *Hybrid Systems: Computation and Control, LNCS 2993*, Springer-Verlag, pp. 129–132.

Asarin, E., Dang, T., Frehse, G., Girard, A., Le Guernic, C., and Maler, O. (2006), "Recent Progress in Continuous and Hybrid Reachability Analysis," in *Proceedings of IEEE International Symposium on Computer-Aided Control Systems Design*, Oct., Munich, Germany.

Aubin, J.P., *Viability Theory*, Systems and Control: Foundations and Applications, Boston, MA: Birkhäuser (1991).

Bayen, A., Mitchell, I., Oishi, M., and Tomlin, C. (2007), "Aircraft Autolander Safety Analysis Through Optimal Control-Based Reach Set Computation," *Journal of Guidance, Control, and Dynamics*, 30, 68–77.

Bryson, A., *Control of Spacecraft and Aircraft*, Princeton Univ. Press (1994).

Cardaliaguet, P., Quincampoix, M., and Saint-Pierre, P. (1999), "Set-valued numerical analysis for optimal control and differential games," in *Stochastic and Differential Games: Theory and Numerical Methods*, eds. M. Bardi, T. Raghavan and T. Parthasarathy, no. 4 in Annals of the International Society of Dynamic Games, Boston, MA: Birkhäuser, pp. 177–247.

Evans, L., and Souganidis, P. (1984), "Differential games and representation formulas for solutions of Hamilton-Jaconbi-Isaacs Equations," *Indiana University Mathematics Journal*, 33, 773–797.

Gao, Y., Lygeros, J., and Quincampoix, M. (2006), "The reachability problem for uncertain hybrid systems revisited: a viability theory perspective," in *Hybrid Systems: Computation and Control, LNCS 3927*, eds. J. Hespanha and A. Tiwari, Berlin Heidelberg: Springer-Verlag, pp. 242–256.

Girard, A., Le Guernic, C., and Maler, O. (2006), "Efficient computation of reachable sets of linear time-invariant systems with inputs," in *Hybrid Systems: Computation and Control, LNCS 3927*, eds. J. Hespanha and A. Tiwari, Springer-Verlag, pp. 257–271.

Girard, A., and Le Guernic, C. (2008), "Efficient reachability analysis for linear systems using support functions," in *IFAC World Congress*, Jul., Seoul, Korea.

Girard, A., and Pappas, G.J. (2007), "Approximation Metrics for Discrete and Continuous Systems," *IEEE Transactions on Automatic Control*, 52, 782–798.

Golub, G.H., and Loan, C.F.V., *Matrix Computations*, Johns Hopkins Univ. Press (1996).

Han, Z., and Krogh, B. (2004), "Reachability Analysis of Hybrid Control Systems Using Reduced-Order Models," in *Proceedings of American Control Conference*, Jun., Boston, MA, pp. 1183–1189.

Han, Z., and Krogh, B.H. (2005), "Reachability Analysis for Affine Systems Using ϵ-Decomposition," in *Proceedings of IEEE Conference on Decision and Control, and European Control Conference*, Dec., Seville, Spain, pp. 6984–6990.

Han, Z., and Krogh, B.H. (2006), "Reachability Analysis of Large-Scale Affine Systems Using Low-Dimensional Polytopes," in *Hybrid Systems: Computation and Control, LNCS 3927*, eds. J. Hespanha and A. Tiwari, Berlin, Germany: Springer-Verlag, pp. 287–301.

Ioannou, P., and Sun, J., *Robust Adaptive Control*, Englewood Cliffs, NJ: Prentice Hall (1996).

Krogh, B.H., and Stursberg, O. (2003), "Efficient Representation and Computation of Reachable Sets for Hybrid Systems," in *Hybrid Systems: Computation and Control, LNCS 2623*, eds. O. Maler and A. Pnueli, Berlin, Germany: Springer-Verlag, pp. 482–497.

Kurzhanski, A.B., and Varaiya, P. (2002), "On Reachability Under Uncertainty," *SIAM Journal on Control and Optimization*, 41, 181–216.

Kurzhanski, A.B., and Varaiya, P. (2000), "Ellipsoidal Techniques for Reachability Analysis," in *Hybrid Systems: Computation and Control, LNCS 1790*, eds. N. Lynch and B. Krogh, Berlin Heidelberg: Springer-Verlag, pp. 202–214.

Kurzhanskiy, A.A., and Varaiya, P. (2007), "Ellipsoidal Techniques for Reachability Analysis of

Discrete-Time Linear Systems," *IEEE Transactions on Automatic Control*, 52, 26–38.

Kvasnica, M., Grieder, P., Baotić, M., and Morari, M. (2004), "Multi-Parametric Toolbox (MPT)," in *Hybrid Systems: Computation and Control, LNCS 2993*, eds. R. Alur and G.J. Pappas, Berlin, Germany: Springer, pp. 448–462.

Lygeros, J., Tomlin, C., and Sastry, S. (1999), "Controllers for reachability specifications for hybrid systems," *Automatica*, 35, 349–370.

Mahmoud, M., and Singh, M., *Large Scale Systems Modelling*, Pergamon Press (1981).

Mitchell, I., and Tomlin, C. (2003), "Overapproximating Reachable Sets by Hamilton-Jacobi Projections," *Journal of Scientific Computing*, 19, 323–346.

Mitchell, I.M. (2007), "A Toolbox of Level Set Methods," Technical report TR-2007-11, UBC Department of Computer Science.

Mitchell, I. (2007), "Comparing Forward and Backward Reachability as Tools for Safety Analysis," in *Hybrid Systems: Computation and Control, LNCS 4416*, eds. A. Bemporad, A. Bicchi and G. Buttazzo, Berlin Heidelberg: Springer-Verlag, pp. 428–443.

Mitchell, I., Bayen, A., and Tomlin, C. (2005), "A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games," *IEEE Transactions on Automatic Control*, 50, 947–957.

Safonov, M.G., and Chiang, R.Y. (1989), "A Schur Method for Balanced-Truncation Model Reduction," *IEEE Transactions on Automatic Control*, 34, 729–733.

Saint-Pierre, P. (2002), "Hybrid kernels and capture basins for impulse constrained systems," in *Hybrid Systems: Computation and Control, LNCS 2289*, eds. C. Tomlin and M. Greenstreet, Berlin Heidelberg: Springer-Verlag, pp. 378–392.

Shishido, N., and Tomlin, C. (2000), "Ellipsoidal Approximations of Reachable Sets for Linear Games," in *Proceedings of IEEE Conference on Decision and Control*, Dec., Sydney, Australia, pp. 999–1004.

Siret, J.M., Michailesco, G., and Bertrand, P. (1977), "Optimal approximation of high-order systems subject to polynomial inputs," *International Journal of Control*, 26, 963–971.

Skogestad, S., and Postlethwaite, I., *Multivariable Feedback Control; Analysis and Design*, West Sussex, UK: John Wiley & Sons (2007).

Stipanović, D., Hwang, I., and Tomlin, C. (2003), "Computation of an Over-Approximation of the Backward Reachable Set using Subsystem Level Set Functions," in *Proceedings of IEE European Control Conference*, Sep., Cambridge, UK.

Strang, G., *Linear Algebra and Its Applications*, Brooks Cole (1988).

Tomlin, C., Mitchell, I., Bayen, A., and Oishi, M. (2003), "Computational techniques for the verification and control of hybrid systems," *Proceedings of the IEEE*, 91, 986–1001.

Tomlin, C., Lygeros, J., and Sastry, S. (2000), "A game theoretic approach to controller design for hybrid systems," *Proceedings of the IEEE*, 88, 949–970.

Varaiya, P. (1998), "Reach set computation using optimal control," in *Proceedings of KIT Workshop on Verification of Hybrid Systems*, Verimag, Grenoble.

Yazarel, H., and Pappas, G.J. (2004), "Geometric programming relaxations for linear system reachability," in *Proceedings of American Control Conference*, Jun., Boston, MA, pp. 553–559.

Zhou, K., Doyle, J.C., and Glover, K., *Robust and Optimal Control*, Englewood Cliffs, NJ: Prentice Hall (1996).

Appendix A: Proof of Proposition 3.6

To prove Proposition 3.6 let us first state a simple lemma.

Lemma A.1: *Denote by* $\mathcal{X}^{\mathfrak{C}}_{[t,\,0]}$ *the backward reachable set of* (3) *over the time interval* $[t, 0]$, $t \in [-\tau, 0]$, $\tau > 0$, *and by* $\mathcal{X}^{\mathfrak{A}}_{[t,\,0]}$ *the backward reachable set of its corresponding autonomous*

system

$$\dot{x} = Ax. \tag{A1}$$

The following inclusions hold:

$$\mathcal{X}_0 \subseteq \mathcal{X}^{\mathfrak{C}}_{[t,\,0]} \subseteq \mathcal{X}^{\mathfrak{A}}_{[t,\,0]} \quad \forall t \in [-\tau, 0]. \tag{A2}$$

Proof Assume, without loss of generality, that $\mathcal{U}$ is a compact hyper-rectangular subset of $\mathbb{R}^p$ such that $\mathcal{U} = \prod_{i=1}^{p} \mathcal{U}_i$, $u_i \in \mathcal{U}_i = [\underline{\mathcal{U}}_i, \overline{\mathcal{U}}_i]$, $0 \in \mathcal{U}_i$. Notice that the autonomous system (A1) is equivalent to the controlled system (3) when $\gamma := \sup_{v\in\mathcal{U}}\|v\|$ is zero. As such, we draw on the level set formulation of the backward reachable set of system (3) and treat (A1) as a particular form of (3) in which the control input u is diminished.

It is well-known (Mitchell et al. 2005) that if $\mathcal{X}_0$ is represented as the zero sublevel set of some bounded and Lipschitz continuous implicit surface function $g\colon \mathbb{R}^n \to \mathbb{R}$, i.e. $\mathcal{X}_0 = \{x \mid g(x) \leq 0\}$, then the backward reachable set $\mathcal{X}^{\mathfrak{C}}_{[t,\,0]}$ can be obtained as the zero sublevel set of the viscosity solution $\phi^{\mathfrak{C}}\colon \mathbb{R}^n \times [-\tau, 0] \to \mathbb{R}$ of the modified terminal value HJB PDE

$$\nabla_t \phi^{\mathfrak{C}}(x,t) = -\min\left\{0, H\left(x, \nabla_x \phi^{\mathfrak{C}}(x,t)\right)\right\}, \quad \phi^{\mathfrak{C}}(x,0) = g(x) \tag{A3}$$

$$H(x,\ell) = \sup_{u\in\mathcal{U}} \left\langle \ell, Ax + Bu \right\rangle \tag{A4}$$

with the Hamiltonian $H(\cdot,\cdot)$ and the costate vector ℓ. Here, $\langle\cdot,\cdot\rangle$ denotes the inner product. Thus, $\mathcal{X}^{\mathfrak{C}}_{[t,\,0]} = \{x \mid \phi^{\mathfrak{C}}(x,t) \leq 0\}$. The optimal Hamiltonian, in this case, can be determined analytically as

$$H^*(x,\ell) = \ell^T Ax + \ell^T Bu^*, \quad u^* = [u_1^* \cdots u_p^*]^T \tag{A5}$$

with

$$u_i^* = \begin{cases} \underline{\mathcal{U}}_i & \text{if} \quad \ell^T b_i < 0; \\ [\underline{\mathcal{U}}_i, \overline{\mathcal{U}}_i] & \text{if} \quad \ell^T b_i = 0; \\ \overline{\mathcal{U}}_i & \text{if} \quad \ell^T b_i > 0 \end{cases}, \quad i = 1, \ldots, p \tag{A6}$$

where b_i is the i-th column vector of matrix B. Notice that the second term on the right hand side of (A5) is always non-negative, i.e. $\ell^T Bu^* \geq 0$. Therefore we have

$$\nabla_t \phi^{\mathfrak{C}}(x,t) = \begin{cases} 0 & \text{if} \quad \ell^T Ax \geq -\ell^T Bu^*; \\ |\ell^T Ax| - \ell^T Bu^* & \text{otherwise.} \end{cases} \tag{A7}$$

When $\gamma \leftarrow 0$, the controlled system (3) is equivalent to the autonomous system (A1) and the Hamiltonian (A4) becomes $H(x,\ell) = H^*(x,\ell) = \ell^T Ax$. Consequently, (A7) reduces to

$$\nabla_t \phi^{\mathfrak{C}}(x,t)\Big|_{\gamma\leftarrow 0} =: \nabla_t \phi^{\mathfrak{A}}(x,t) = \begin{cases} 0 & \text{if} \quad \ell^T Ax \geq 0; \\ |\ell^T Ax| & \text{otherwise} \end{cases} \tag{A8}$$

where $\phi^{\mathfrak{A}}(\cdot,\cdot)$ is to denote the implicit surface function whose zero sublevel set determines the backward reachable set $\mathcal{X}^{\mathfrak{A}}_{[t,\,0]}$ of (A1). That is, $\mathcal{X}^{\mathfrak{A}}_{[t,\,0]} = \{x \mid \phi^{\mathfrak{A}}(x,t) \leq 0\}$.

Comparing (A7) and (A8) one can observe that not only the interval over which $\nabla_t\phi$ (the rate of surface change in time) is zero is shortened (i.e. $\ell^T Ax \geq 0$ as opposed to $\ell^T Ax \geq -\ell^T Bu^*$),

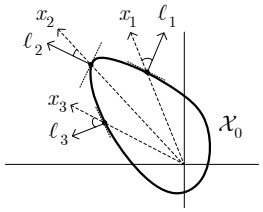


Figure A1. Three sample costate vectors (ℓ_i) and trajectories (x_i) initiating from the boundary of an arbitrarily-shaped convex target set $\mathcal{X}_0$ in the phase-plane of a simple planar system in forward time. Notice the non-negativity of $\langle \ell_i, x_i \rangle$ as shown in forward time. In backward time the trajectories are reversed and the eigenvalues are negated, hence the Hamiltonian is still non-negative.

but also its maximum (positive) value is increased (i.e. $|\ell^T A x|$ as opposed to $|\ell^T A x| - \ell^T B u^*$). Therefore, for all $(x,t) \in \mathbb{R}^n \times [-\tau, 0]$ we have

$$\nabla_t \phi^{\mathfrak{A}}(x,t) \geq \nabla_t \phi^{\mathfrak{C}}(x,t) \tag{A9}$$

$$\Rightarrow \;\; \phi^{\mathfrak{A}}(x,t) \leq \phi^{\mathfrak{C}}(x,t) \leq \phi^{\mathfrak{A},\mathfrak{C}}(x,0) \leq 0 \tag{A10}$$

$$\Leftrightarrow \;\; \mathcal{X}^{\mathfrak{A}}_{[t,\,0]} \supseteq \mathcal{X}^{\mathfrak{C}}_{[t,\,0]} \supseteq \mathcal{X}_0. \tag{A11}$$

□

Notice that this result agrees with the intuitive interpretation that larger control authority (i.e. $\gamma \neq 0$) implies a smaller *unsafe* reachable set. We are now ready to prove Proposition 3.6.

Proof [Proof of Proposition 3.6] Using Lemma A.1 we have $\mathcal{X}^{\mathfrak{A}}_{[t,\,0]} \supseteq \mathcal{X}^{\mathfrak{C}}_{[t,\,0]}$, where $\mathcal{X}^{\mathfrak{A}}_{[t,\,0]}$ denotes the backward reachable set of the autonomous system (A1). Therefore, to prove $\mathcal{X}^{\mathfrak{C}}_{[t,\,0]} = \mathcal{X}_0$, $\forall t \in [-\tau, 0]$, it is sufficient to show that $\mathcal{X}^{\mathfrak{A}}_{[t,\,0]} = \mathcal{X}_0$, $\forall t \in [-\tau, 0]$.

Let $S\Lambda S^{-1}$ be the eigen-decomposition of A. Conditions (ii) and (iii) imply $\Lambda = \lambda I_n$, $\lambda \geq 0$. Rewriting the Hamiltonian of the HJB PDE (A3) for the autonomous system (A1) and using condition (i) we have

$$H(x, \nabla_x \phi^{\mathfrak{A}}(x,t)) = \big\langle \nabla_x \phi^{\mathfrak{A}}(x,t), Ax \big\rangle \tag{A12}$$

$$= \big\langle \nabla_x \phi^{\mathfrak{A}}(x,t), S\Lambda S^{-1} x \big\rangle \tag{A13}$$

$$= \lambda \big\langle \nabla_x \phi^{\mathfrak{A}}(x,t), x \big\rangle \geq 0 \qquad \forall (x,t) \in \mathbb{R}^n \times [-\tau, 0]. \tag{A14}$$

The non-negativity of the Hamiltonian is due to the fact that $\mathcal{X}_0$ is convex and $\mathbf{0} \in \operatorname{int} \mathcal{X}_0$. Thus, the costate vector $\nabla_x \phi^{\mathfrak{A}}(x,t)$ at every point on the boundary constitutes an acute (hyper-) angle with respect to the trajectory x initiating from that point in forward time. This is schematically illustrated for a trivial planar system in Figure A1. As a result, for all $(x,t) \in \mathbb{R}^n \times [-\tau, 0]$ we have

$$H(x, \nabla_x \phi^{\mathfrak{A}}(x,t)) \geq 0 \Leftrightarrow \nabla_t \phi^{\mathfrak{A}}(x,t) = 0 \tag{A15}$$

$$\Leftrightarrow \mathcal{X}^{\mathfrak{A}}_{[t,\,0]} = \mathcal{X}_0. \tag{A16}$$

This concludes the proof. □