UNIVERSITY OF OSLO
Department of Informatics

Static Analysis of SPDIs for State-Space Reduction

Research Report No. 336

Gordon Pace

Gerardo Schneider

Isbn 82-7368-291-9
Issn 0806-3036

April 2006

Static Analysis of SPDIs for State-Space Reduction

Gordon Pace* Gerardo Schneider†

April 2006

Abstract

Polygonal hybrid systems (SPDI) are a subclass of planar hybrid automata which can be represented by piecewise constant differential inclusions. The reachability problem as well as the computation of certain objects of the phase portrait, namely the viability, controllability and invariance kernels, for such systems is decidable. In this paper we show how to compute another object of an SPDI phase portrait, namely semi-separatrix curves and show how the phase portrait can be used for reducing the state-space for optimizing the reachability analysis.

1 Introduction

Hybrid systems combining discrete and continuous dynamics arise as mathematical models of various artificial and natural systems, and as approximations to complex continuous systems. They have been used in various domains, including avionics, robotics and bioinformatics. Reachability analysis has been the principal research question in the verification of hybrid systems, even if it is a well-known result that for most non-trivial subclasses of hybrid systems reachability and most verification questions are undecidable. Various decidable subclasses have, subsequently, been identified, including timed [AD94] and rectangular automata [HKPV95], hybrid automata with linear

*Dept. of Computer Science and AI, University of Malta, Msida, Malta. E-mail: gordon.pace@um.edu.mt

†Dept. of Informatics – Univ. of Oslo, P.O. Box 1080 Blindern, N-0316 Oslo, Norway. E-mail: gerardo@ifi.uio.no

vector fields [LPY01], piecewise constant derivative systems (PCDs) [MP93] and polygonal differential inclusion systems (SPDIs) [ASY01].

Compared to reachability verification, qualitative analysis of hybrid systems is a relatively neglected area [ALQ^{+}01b, DV95, KdB01, MS00, SP02, SJSL00]. Typical qualitative questions include: "Are there 'sink' regions where a trajectory can never leave once it enters the region?"; "Which are the basins of attraction of such regions?"; "Are there regions in which every point in the region is reachable from every other point in the region without leaving it?". To answer such questions one usually gives a collection of objects characterizing these sets, hence providing useful information about the qualitative behavior of the hybrid system. The set of all such objects for a given system is called the *phase portrait* of the system.

Defining and constructing phase portraits of hybrid systems has been directly addressed for PCDs in [MS00], and for SPDIs in [ASY02]. In this paper we present a a new element of the phase portrait for SPDIs, and discuss how the phase portrait can be used to reduce the size of an SPDI, as an aid to verification.

Roughly speaking, an *SPDI* (Fig. 1) is a finite partition $\mathbb{P}$ of the plane (into convex polygonal areas), and, for each $P \in \mathbb{P}$ an associated pair of vectors $\mathbf{a}_P$ and $\mathbf{b}_P$. The SPDI behaviour is defined by the differential inclusion $\dot{\mathbf{x}} \in \angle_{\mathbf{a}_P}^{\mathbf{b}_P}$ for $\mathbf{x} \in P$, where $\angle_{\mathbf{a}}^{\mathbf{b}}$ denotes the angle on the plane between the vectors $\mathbf{a}$ and $\mathbf{b}$.

In [ASY01] it has been proved that edge-to-edge and polygon-to-polygon reachability in SPDIs is decidable by exploiting the topological properties of the plane. The procedure is not based on the computation of the reach-set but rather on the exploration of a finite number of types of qualitative behaviors obtained from the edge-signatures of trajectories (the sequences of their intersections with the edges of the polygons). Such types of signatures may contain loops which can be very expensive (or impossible) to explore naively. However, it has been shown that loops have structural properties that are exploited by the algorithm to efficiently compute the effect of such loops. In summary, the novelty of the approach is the combination of several techniques, namely, (i) the representation of the two-dimensional continuous dynamics as a one-dimensional discrete dynamical system, (ii) the characterization of the set of qualitative behaviors of the latter as a finite set of types of signatures, and (iii) the "acceleration" of the iterations in the case of cyclic signatures.

Given a cycle on a SPDI, we can speak about a number of kernels pertaining to that cycle. The *viability* kernel is the largest set of points in the cycle which may loop forever within the cycle. The *controllability* kernel is the largest set of strongly connected points in the cycle (such that any point in the set may

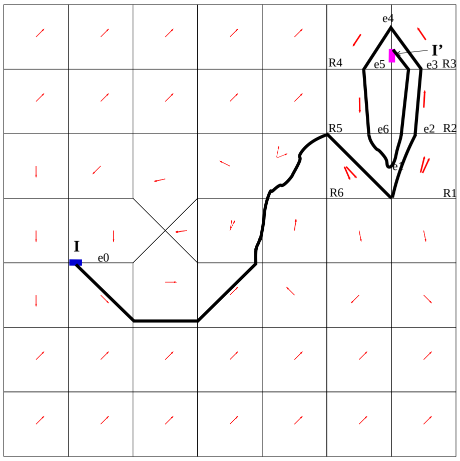


Figure 1: An SPDI and its trajectory segment.

be reached from any other). An *invariant set* is a set of points such that each point must keep rotating within the set forever. The *invariance kernel* is the largest of such sets. The information gathered for computing reachability turns out to be useful for computing viability, controllability and invariance kernels of such systems. Algorithms for computing these kernels have been presented in [ASY02, Sch04] and implemented in the tool set SPeeDI$^+$[PS06]. The contribution of this paper is threefold. We start by giving an algorithm to compute *semi-separatrix curves* (or simply, *semi-separatrices*) of SPDIs. Separatrices are convex polygons dissecting the plane into two mutually non-reachable subsets. The notion of separatrix can be relaxed, obtaining *semi-separatrix curves*, such that some points in one set may be reachable from the other set, but not vice-versa. We then show how the kernels can be used to answer reachability questions directly. We also show how semi-separatrices can be used to optimize the reachability algorithm for SPDIs by reducing the number of states of the SPDI graph. The optimization is based on topological properties of the plane (and in particular, that of SPDIs).

The paper is structured as follows. In the next section we introduce the necessary theoretical background, including the definition of SPDI, kernels and semi-separatrices as well as how to compute such phase portrait objects. In Section 3 we show how the semi-separatrices can be used for reducing the state-space of the reachability graph whereas in Section 4 we present the optimization done by using the kernels.

2 Theoretical Background

A (positive) *affine* function $f : \mathbb{R} \rightarrow \mathbb{R}$ is such that $f(x) = ax + b$ with $a > 0$. An *affine multivalued* function $F : \mathbb{R} \rightarrow 2^{\mathbb{R}}$, denoted $F = \langle f_l, f_u \rangle$, is defined by $F(x) = \langle f_l(x), f_u(x) \rangle$ where f_l and f_u are affine and $\langle \cdot, \cdot \rangle$ denotes an interval. For notational convenience, we do not make explicit whether intervals are open, closed, left-open or right-open, unless required for comprehension. For an interval $I = \langle l, u \rangle$ we have that $F(\langle l, u \rangle) = \langle f_l(l), f_u(u) \rangle$. The *inverse* of F is defined by $F^{-1}(x) = \{y \mid x \in F(y)\}$. The *universal inverse* of F is defined by $\tilde{F}^{-1}(I) = I'$ if and only if I' is the greatest non-empty interval such that for all $x \in I'$, $F(x) \subseteq I$.

It is not difficult to show that $F^{-1} = \langle f_u^{-1}, f_l^{-1} \rangle$ and similarly that $\tilde{F}^{-1} = \langle f_l^{-1}, f_u^{-1} \rangle$, provided that $\langle f_l^{-1}, f_u^{-1} \rangle \neq \emptyset$. Notice that if I is a singleton then $\tilde{F}^{-1}$ is defined only if $f_l = f_u$. These classes of functions are closed under composition.

A *truncated affine multivalued* function (TAMF) $\mathcal{F} : \mathbb{R} \rightarrow 2^{\mathbb{R}}$ is defined by an affine multivalued function F and intervals $S \subseteq \mathbb{R}^+$ and $J \subseteq \mathbb{R}^+$ as follows: $\mathcal{F}(x) = F(x) \cap J$ if $x \in S$, otherwise $\mathcal{F}(x) = \emptyset$. For convenience we write $\mathcal{F}(x) = F(\{x\} \cap S) \cap J$. For an interval I, $\mathcal{F}(I) = F(I \cap S) \cap J$ and $\mathcal{F}^{-1}(I) = F^{-1}(I \cap J) \cap S$. The *universal inverse* of $\mathcal{F}$ is defined by $\tilde{\mathcal{F}}^{-1}(I) = I'$ if and only if I' is the greatest non-empty interval such that for all $x \in I'$, $F(x) \subseteq I$ and $F(x) = \mathcal{F}(x)$.

We say that $\mathcal{F}$ is *normalized* if $S = \mathsf{Dom}\mathcal{F} = \{x \mid F(x) \cap J \neq \emptyset\}$ (thus, $S \subseteq F^{-1}(J)$) and $J = \mathsf{Im}\mathcal{F} = \mathcal{F}(S)$.

The following theorem states that TAMFs are closed under composition [ASY01].

Theorem 1. The composition of two TAMFs $\mathcal{F}_1(I) = F_1(I \cap S_1) \cap J_1$ and $\mathcal{F}_2(I) = F_2(I \cap S_2) \cap J_2$, is the TAMF $(\mathcal{F}_2 \circ \mathcal{F}_1)(I) = \mathcal{F}(I) = F(I \cap S) \cap J$, where $F = F_2 \circ F_1$, $S = S_1 \cap F_1^{-1}(J_1 \cap S_2)$ and $J = J_2 \cap F_2(J_1 \cap S_2)$. □

2.1 SPDI

An *angle* $\angle_{\mathbf{a}}^{\mathbf{b}}$ on the plane, defined by two non-zero vectors $\mathbf{a}, \mathbf{b}$ is the set of all positive linear combinations $\mathbf{x} = \alpha\ \mathbf{a} + \beta\ \mathbf{b}$, with $\alpha, \beta \geq 0$, and $\alpha + \beta > 0$. We can always assume that $\mathbf{b}$ is situated in the counter-clockwise direction from $\mathbf{a}$.

A *polygonal hybrid system*[1] (SPDI) is defined by giving a finite partition $\mathbb{P}$ of the plane into convex polygonal sets, and associating with each $P \in \mathbb{P}$ a

[1] In the literature the names *polygonal differential inclusion* and *simple planar differential inclusion* have been used to describe the same systems.

couple of vectors $\mathbf{a}_P$ and $\mathbf{b}_P$. Let $\phi(P) = \angle_{\mathbf{a}_P}^{\mathbf{b}_P}$. The SPDI is determined by $\dot{\mathbf{x}} \in \phi(P)$ for $\mathbf{x} \in P$.

Let $E(P)$ be the set of edges of P. We say that e is an *entry* of P if for all $\mathbf{x} \in e$ and for all $\mathbf{c} \in \phi(P)$, $\mathbf{x} + \mathbf{c}\epsilon \in P$ for some $\epsilon > 0$. We say that e is an *exit* of P if the same condition holds for some $\epsilon < 0$. We denote by $\mathit{in}(P) \subseteq E(P)$ the set of all entries of P and by $\mathit{out}(P) \subseteq E(P)$ the set of all exits of P.

Assumption 1. *All the edges in $E(P)$ are either entries or exits, that is, $E(P) = \mathit{in}(P) \cup \mathit{out}(P)$.*

A *trajectory segment* of an SPDI is a continuous function $\xi : [0, T] \to \mathbb{R}^2$ which is smooth everywhere except in a discrete set of points, and such that for all $t \in [0, T]$, if $\xi(t) \in P$ and $\dot{\xi}(t)$ is defined then $\dot{\xi}(t) \in \phi(P)$. The *signature*, denoted $\mathsf{Sig}(\xi)$, is the ordered sequence of edges traversed by the trajectory segment, that is, $e_1, e_2, \ldots$, where $\xi(t_i) \in e_i$ and $t_i < t_{i+1}$. If $T = \infty$, a trajectory segment is called a *trajectory.*

Example 1. Consider the SPDI illustrated in Fig. 1. For sake of simplicity we will only show the dynamics associated to regions R_1 to R_6 in the picture. For each region R_i, $1 \leq i \leq 6$, there is a pair of vectors $(\mathbf{a}_i, \mathbf{b}_i)$, where: $\mathbf{a}_1 = (45, 100), \mathbf{b}_1 = (1, 4)$, $\mathbf{a}_2 = \mathbf{b}_2 = (1, 10)$, $\mathbf{a}_3 = \mathbf{b}_3 = (-2, 3)$, $\mathbf{a}_4 = \mathbf{b}_4 = (-2, -3)$, $\mathbf{a}_5 = \mathbf{b}_5 = (1, -15)$, $\mathbf{a}_6 = (1, -2), \mathbf{b}_6 = (1, -1)$.

A trajectory segment starting on interval $I \subset e_0$ and finishing in interval $I' \subseteq e_4$ is depicted. ■

Definition 1. *We say that a signature σ is* feasible *if and only if there exists a trajectory segment ξ with signature σ, i.e., $\mathsf{Sig}(\xi) = \sigma$.* ■

From this definition, it immediately follows that extending an unfeasible signature, can never make it feasible:

Proposition 1. *If a signature σ is not feasible, then neither is any extension of the signature — for any signatures σ' and σ'', the signature $\sigma'\sigma\sigma''$ is not feasible.* □

Given an SPDI $\mathcal{S}$, let $\mathcal{E}$ be the set of edges of $\mathcal{S}$, then we can define a graph $\mathcal{G}_\mathcal{S}$ where nodes correspond to edges of $\mathcal{S}$ and such that there exists an arc from one node to another if there exists a trajectory segment from the first edge to the second one without traversing any other edge. More formally:

Definition 2. *Given an SPDI $\mathcal{S}$, the* underlying graph of $\mathcal{S}$ *(or simply the* graph of $\mathcal{S}$*), is a graph $\mathcal{G}_\mathcal{S} = (N_\mathcal{G}, A_\mathcal{G})$, with $N_\mathcal{G} = \mathcal{E}$ and $A_\mathcal{G} = \{(e, e') \mid \exists \xi, t \,.\, \xi(0) \in e \wedge \xi(t) \in e' \wedge \mathsf{Sig}(\xi) = ee'\}$. We say that a sequence $e_0 e_1 \ldots e_k$ of nodes in $\mathcal{G}_\mathcal{S}$ is a* path *whenever $(e_i, e_{i+1}) \in A_\mathcal{G}$ for $0 \leq i \leq k - 1$.* ■

The following lemma shows the relation between edge signatures in an SPDI and paths in its corresponding graph.

Lemma 2. *If ξ is a trajectory segment of $\mathcal{S}$ with edge signature $\mathsf{Sig}(\xi) = \sigma = e_0 \ldots e_p$, it follows that σ is a path in $\mathcal{G}_{\mathcal{S}}$.* □

Remark. Notice that the converse of the above lemma is not true in general. It is possible to find a counter-example where there exists a path from node e to e', but it does not exist a trajectory segment form edge e to edge e' on the SPDI.

Lemma 3. *If $\sigma = e_0 \ldots e_p$ is a feasible signature, then σ is a path in $\mathcal{G}_{\mathcal{S}}$.* □

2.2 Successors and predecessors

Given an SPDI, we fix a one-dimensional coordinate system on each edge to represent points laying on edges [ASY01]. For notational convenience, we indistinctly use letter e to denote the edge or its one-dimensional representation. Accordingly, we write $\mathbf{x} \in e$ or $x \in e$, to mean "point $\mathbf{x}$ in edge e with coordinate x in the one-dimensional coordinate system of e". The same convention is applied to sets of points of e represented as intervals (e.g., $\mathbf{x} \in I$ or $x \in I$, where $I \subseteq e$) and to trajectories (e.g., "ξ starting in x" or "ξ starting in $\mathbf{x}$").
Now, let $P \in \mathbb{P}$, $e \in \mathit{in}(P)$ and $e' \in \mathit{out}(P)$. For $I \subseteq e$, $\mathsf{Succ}_{e,e'}(I)$ is the set of all points in e' reachable from some point in I by a trajectory segment $\xi : [0,t] \to \mathbb{R}^2$ in P (i.e., $\xi(0) \in I \wedge \xi(t) \in e' \wedge \mathsf{Sig}(\xi) = ee'$). It has been shown [ASY01] that $\mathsf{Succ}_{e,e'}$ is a TAMF.

Example 2. Let $e_1, \ldots, e_6$ be as in Fig. 1 and $I = [l, u]$. We assume a one-dimensional coordinate system. We have:

$$\begin{aligned}
F_{e_1e_2}(I) &= \left[\frac{l}{4}, \frac{9}{20}u\right], & S &= [0,10], & J &= \left[0, \frac{9}{2}\right] \\
F_{e_2e_3}(I) &= [l+1, u+1], & S &= [0,9], & J &= [1,10] \\
F_{e_3e_4}(I) &= \left[\frac{3}{2}l, \frac{3}{2}u\right], & S &= \left[0, \frac{20}{3}\right], & J &= [0,10] \\
F_{e_4e_5}(I) &= \left[\frac{2}{3}l, \frac{2}{3}u\right], & S &= [0,10], & J &= \left[0, \frac{20}{3}\right] \\
F_{e_5e_6}(I) &= \left[l - \frac{2}{3}, u - \frac{2}{3}\right], & S &= \left[\frac{2}{3}, 10\right], & J &= \left[0, \frac{28}{3}\right] \\
F_{e_6e_1}(I) &= [l, 2u], & S &= [0,10], & J &= [0,10]
\end{aligned}$$

with $\mathsf{Succ}_{e_ie_{i+1}}(I) = F_{e_ie_{i+1}}(I \cap S_i) \cap J_{i+1}$, for $1 \leq i \leq 5$, and $\mathsf{Succ}_{e_6e_1}(I) = F_{e_6e_1}(I \cap S_6) \cap J_1$. ■

Given a sequence $w = e_1, e_2, \ldots, e_n$, Theorem 1 implies that the successor of I along w defined as $\mathsf{Succ}_w(I) = \mathsf{Succ}_{e_{n-1},e_n} \circ \ldots \circ \mathsf{Succ}_{e_1,e_2}(I)$ is a TAMF.

Example 3. Let $\sigma = e_1 \cdots e_6e_1$. It results that $\mathsf{Succ}_\sigma(I) = F(I \cap S) \cap J$, where:

$$F(I) \;=\; \left[\frac{l}{4} + \frac{1}{3}, \frac{9}{10}u + \frac{2}{3}\right] \tag{1}$$

$S = [\frac{37}{25}e^{-16}, 10]$ and $J = [\frac{1}{3}, \frac{29}{3}]$ are computed using Theorem 1. ■

For $I \subseteq e'$, $\mathsf{Pre}_{e,e'}(I)$ is the set of points in e that can reach a point in I by a trajectory segment in P. The $\forall$*-predecessor* $\widetilde{\mathsf{Pre}}(I)$ is defined in a similar way to $\mathsf{Pre}(I)$ using the universal inverse instead of just the inverse: For $I \subseteq e'$, $\widetilde{\mathsf{Pre}}_{ee'}(I)$ is the set of points in e such that *any* successor of such points are in I by a trajectory segment in P. Both definitions can be extended straightforwardly to signatures $\sigma = e_1 \cdots e_n$: $\mathsf{Pre}_\sigma(I)$ and $\widetilde{\mathsf{Pre}}_\sigma(I)$. Therefore, the successor operator has two inverse operators.

Example 4. Let $\sigma = e_1 \ldots e_6e_1$ be as in Fig. 1 and $I = [l, u]$. Now, $\mathsf{Pre}_{e_ie_{i+1}}(I) = F^{-1}_{e_ie_{i+1}}(I \cap J_{i+1}) \cap S_i$, for $1 \leq i \leq 5$, and $\mathsf{Pre}_{e_6e_1}(I) = F^{-1}_{e_6e_1}(I \cap J_1) \cap S_6$, where:

$$\begin{aligned} F^{-1}_{e_1e_2}(I) &= \left[\frac{20}{9}l, 4u\right] & F^{-1}_{e_2e_3}(I) &= [l-1, u-1] \\ F^{-1}_{e_3e_4}(I) &= \left[\frac{2}{3}l, \frac{2}{3}u\right] & F^{-1}_{e_4e_5}(I) &= \left[\frac{3}{2}l, \frac{3}{2}u\right] \\ F^{-1}_{e_5e_6}(I) &= \left[l + \frac{2}{3}, u + \frac{2}{3}\right] & F^{-1}_{e_6e_1}(I) &= \left[\frac{l}{2}, u\right] \end{aligned}$$

Besides, $\mathsf{Pre}_\sigma(I) = F^{-1}(I \cap J) \cap S$, where $F^{-1}(I) = [\frac{10}{9}l - \frac{20}{27}, 4u - \frac{4}{3}]$. Similarly, we compute $\widetilde{\mathsf{Pre}}_\sigma(I) = \tilde{F}^{-1}(I \cap J) \cap S$, where $\tilde{F}^{-1}(I) = \left[4l - \frac{4}{3}, \frac{10}{9}u - \frac{20}{27}\right]$. ■

2.3 Qualitative analysis of simple edge-cycles

Let $\sigma = e_1 \cdots e_ke_1$ be a simple edge-cycle, i.e., $e_i \neq e_j$ for all $1 \leq i \neq j \leq k$. Let $\mathsf{Succ}_\sigma(I) = F(I \cap S) \cap J$ with $F = \langle f_l, f_u \rangle$ (we suppose that this representation is normalized). We denote by $\mathcal{D}_\sigma$ the one-dimensional discrete-time dynamical system defined by Succ_σ, that is $x_{n+1} \in \mathsf{Succ}_\sigma(x_n)$.

Assumption 2. *None of the two functions f_l, f_u is the identity.*

Let l^* and u^* be the fixpoints[2] of f_l and f_u, respectively, and $S \cap J = \langle L, U \rangle$. A simple cycle is of one of the following types [ASY01]:

STAY. The cycle is not abandoned neither by the leftmost nor the rightmost trajectory, that is, $L \leq l^* \leq u^* \leq U$.

DIE. The rightmost trajectory exits the cycle through the left (consequently the leftmost one also exits) or the leftmost trajectory exits the cycle through the right (consequently the rightmost one also exits), that is, $u^* < L \vee l^* > U$.

EXIT-BOTH. The leftmost trajectory exits the cycle through the left and the rightmost one through the right, that is, $l^* < L \wedge u^* > U$.

EXIT-LEFT. The leftmost trajectory exits the cycle (through the left) but the rightmost one stays inside, that is, $l^* < L \leq u^* \leq U$.

EXIT-RIGHT. The rightmost trajectory exits the cycle (through the right) but the leftmost one stays inside, that is, $L \leq l^* \leq U < u^*$.

Example 5. Let $\sigma = e_1 \cdots e_6 e_1$. We have $S \cap J = \langle L, U \rangle = [\frac{1}{3}, \frac{29}{3}]$. The fixpoints of Eq. (1) are such that $\frac{1}{3} < l^* = \frac{11}{25} < u^* = \frac{20}{3} < \frac{29}{3}$. Thus, σ is a STAY. ■

The classification above gives us some useful information about the qualitative behavior of trajectories. Any trajectory that enters a cycle of type DIE will eventually quit it after a finite number of turns. If the cycle is of type STAY, all trajectories that happen to enter it will keep turning inside it forever. In all other cases, some trajectories will turn for a while and then exit, and others will continue turning forever. This information is crucial for proving decidability of the reachability problem.

Example 6. Consider the SPDI of Fig. 1. Fig. 2 shows part of the reach set of the interval $[8, 10] \subset e_0$, answering positively to the reachability question: Is $[1, 2] \subset e_4$ reachable from $[8, 10] \subset e_0$? Fig. 2 has been automatically generated by the SPeeDi toolbox we have developed for reachability analysis of SPDIs based on the results of [ASY01]. ■

[2] The fixpoint x^* is computed by solving the equation $f(x^*) = x^*$, where $f(\cdot)$ is positive affine.

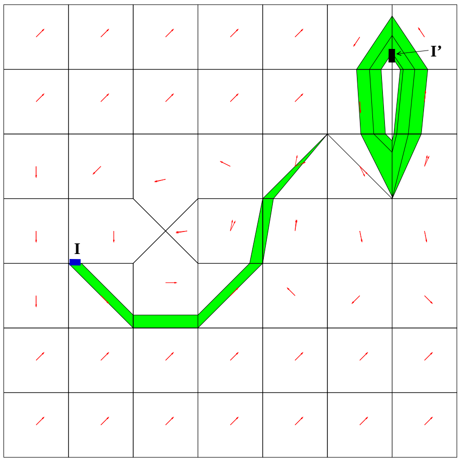


Figure 2: Reachability analysis.

The above result does not allow us to directly answer other questions about the behavior of the SPDI such as determine for a given point (or set of points) whether: (a) there exists (at least) one trajectory that remains in the cycle, and (b) it is possible to control the system to reach any other point. In order to do this, we need to further study the properties of the system around simple edge-cycles.

2.4 Kernels

We can now present how to compute the invariance, controllability and viability kernels of an SPDI. Proofs are omitted but for further details, refer to [ASY02] and [Sch04]. In the following, for K a subset of $\mathbb{R}^2$ and σ a cyclic signature, we define K_σ as follows:

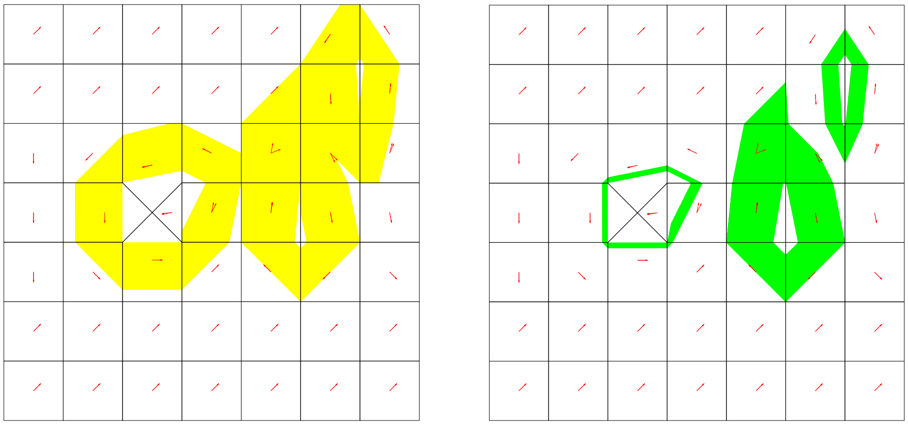
$$K_\sigma \quad = \quad \bigcup_{i=1}^{k} (int(P_i) \cup e_i) \qquad (2)$$

where P_i is such that $e_{i-1} \in in(P_i)$, $e_i \in out(P_i)$ and $int(P_i)$ is P_i's interior.

2.4.1 Viability Kernel

We now recall the definition of *viability kernel* [Aub01].

Definition 3. *A trajectory ξ is* viable *in K if $\xi(t) \in K$ for all $t \geq 0$. K is a* viability domain *if for every $\mathbf{x} \in K$, there exists at least one trajectory*



(a) (b)

Figure 3: (a) Viability Kernels; (b) Controllability Kernels

ξ, with $\xi(0) = \mathbf{x}$, which is viable in K. The viability kernel *of K, denoted* $\mathsf{Viab}(K)$*, is the largest viability domain contained in K.*

For $I \subseteq e_1$ we define $\overline{\mathsf{Pre}}_\sigma(I)$ to be the set of all $\mathbf{x} \in \mathbb{R}^2$ for which there exists a trajectory segment ξ starting in $\mathbf{x}$, that reaches some point in I, such that $\mathsf{Sig}(\xi)$ is a suffix of $e_2 \ldots e_k e_1$. It is easy to see that $\overline{\mathsf{Pre}}_\sigma(I)$ is a polygonal subset of the plane which can be calculated using the following procedure. We start by defining:

$$\overline{\mathsf{Pre}}_e(I) \quad = \quad \{\mathbf{x} \mid \exists \xi : [0,t] \to \mathbb{R}^2, t > 0 \;.\; \xi(0) = \mathbf{x} \wedge \xi(t) \in I \wedge \mathsf{Sig}(\xi) = e\}$$

and apply this operation k times: $\overline{\mathsf{Pre}}_\sigma(I) = \bigcup_{i=1}^{k} \overline{\mathsf{Pre}}_{e_i}(I_i)$ with $I_1 = I$, $I_k = \mathsf{Pre}_{e_k,e_1}(I_1)$ and $I_i = \mathsf{Pre}_{e_i,e_{i+1}}(I_{i+1})$, for $2 \leq i \leq k-1$.
The following result provides a non-iterative algorithmic procedure for computing the viability kernel of K_σ on an SPDI:

Theorem 4. *If σ is not DIE,* $\mathsf{Viab}(K_\sigma) = \overline{\mathsf{Pre}}_\sigma(S)$*, otherwise* $\mathsf{Viab}(K_\sigma) = \emptyset$*.* □

Example 7. *Fig. 3-(a) shows all the viability kernels of the SPDI given in Example 1. There are 4 cycles with viability kernels — in the picture two of the kernels are overlapping.* ■

2.4.2 Controllability Kernel

We say K is *controllable* if for any two points $\mathbf{x}$ and $\mathbf{y}$ in K there exists a trajectory segment ξ starting in $\mathbf{x}$ that reaches an arbitrarily small neighborhood of $\mathbf{y}$ without leaving K. More formally:

Definition 4. *A set K is controllable if $\forall \mathbf{x}, \mathbf{y} \in K, \forall \delta > 0, \exists \xi : [0,t] \to \mathbb{R}^2, t > 0 \ . \ (\xi(0) = \mathbf{x} \wedge |\xi(t) - \mathbf{y}| < \delta \wedge \forall t' \in [0,t] \ . \ \xi(t') \in K)$. The* controllability kernel *of K, denoted $\mathsf{Cntr}(K)$, is the largest controllable subset of K.*

For a given cyclic signature σ, we define $\mathcal{C}_{\mathcal{D}}(\sigma)$ as follows:

$$\mathcal{C}_{\mathcal{D}}(\sigma) = \begin{cases} \langle L, U \rangle & \text{if } \sigma \text{ is EXIT-BOTH} \\ \langle L, u^* \rangle & \text{if } \sigma \text{ is EXIT-LEFT} \\ \langle l^*, U \rangle & \text{if } \sigma \text{ is EXIT-RIGHT} \\ \langle l^*, u^* \rangle & \text{if } \sigma \text{ is STAY} \\ \emptyset & \text{if } \sigma \text{ is DIE} \end{cases} \tag{3}$$

For $I \subseteq e_1$ let us define $\overline{\mathsf{Succ}}_\sigma(I)$ as the set of all points $\mathbf{y} \in \mathbb{R}^2$ for which there exists a trajectory segment ξ starting in some point $x \in I$, that reaches $\mathbf{y}$, such that $\mathsf{Sig}(\xi)$ is a prefix of $e_1 \dots e_k$. The successor $\overline{\mathsf{Succ}}_\sigma(I)$ is a polygonal subset of the plane which can be computed similarly to $\overline{\mathsf{Pre}}_\sigma(I)$. Define

$$\mathcal{C}(\sigma) = (\overline{\mathsf{Succ}}_\sigma \cap \overline{\mathsf{Pre}}_\sigma)(\mathcal{C}_{\mathcal{D}}(\sigma))$$

We compute the controllability kernel of K_σ as follows:

Theorem 5. $\mathsf{Cntr}(K_\sigma) = \mathcal{C}(\sigma)$. □

Example 8. *Fig. 3-(b) shows all the controllability kernels of the SPDI given in Example 1. There are 4 cycles with controllability kernels — in the picture two of the kernels are overlapping.* ■

The following result which relates controllability and viability kernels, states that the viability kernel of a given cycle is the local basin of attraction of the corresponding controllability kernel.

Proposition 2. *Any viable trajectory in K_σ converges to $\mathsf{Cntr}(K_\sigma)$.* □

Let $\mathsf{Cntr}^l(K_\sigma)$ be the closed curve obtained by taking the leftmost trajectory and $\mathsf{Cntr}^u(K_\sigma)$ be the closed curve obtained by taking the rightmost trajectory which can remain inside the controllability kernel. In other words, $\mathsf{Cntr}^l(K_\sigma)$ and $\mathsf{Cntr}^u(K_\sigma)$ are the two polygons defining the controllability kernel.

A non-empty controllability kernel $\mathsf{Cntr}(K_\sigma)$ of a given cyclic signature σ partitions the plane into three disjoint subsets: (1) the controllability kernel itself, (2) the set of points limited by $\mathsf{Cntr}^l(K_\sigma)$ (and not including $\mathsf{Cntr}^l(K_\sigma)$) and (3) the set of points limited by $\mathsf{Cntr}^u(K_\sigma)$ (and not including $\mathsf{Cntr}^u(K_\sigma)$).

Definition 5. *We define the* inner *of* $\mathsf{Cntr}(K_\sigma)$ *(denoted by* $\mathsf{Cntr}_{in}(K_\sigma)$*) to be the subset defined by (2) above if the cycle is counter-clockwise or to be the subset defined by (3) if it is clockwise. The* outer *of* $\mathsf{Cntr}(K_\sigma)$ *(denoted by* $\mathsf{Cntr}_{out}(K_\sigma)$*) is defined to be the subset which is not the inner nor the controllability itself.*

Remark: Notice that an edge in the SPDI may be split into parts by the controllability kernel — part inside, part on the kernel and part outside. In such cases, we can generate a different SPDI, with the same dynamics but with the edge split into parts, such that each part is completely inside, on or outside the kernel. Although the signatures will obviously change, it is trivial to prove that the behaviour of the SPDI remains identical to the original. To simplify presentation, in the rest of the paper, we will assume that all edges are either completely inside, on or completely outside the kernels. We note that in practice splitting is not necessary since we can just consider parts of edges.

Proposition 3. *Given two edges e and e', one lying completely inside a controllability kernel, and the other outside or on the same controllability kernel, such that ee' is feasible, then there exists a point on the controllability kernel, which is reachable from e and from which e' is reachable.*

Proof. Let $e \subseteq \mathsf{Cntr}_{in}(K_\sigma)$. Let us assume that $e' \subseteq \mathsf{Cntr}(K_\sigma)$; since ee' is feasible, by the Jordan curve theorem [Hen79], the trajectory must cross $\mathsf{Cntr}^l(K_\sigma)$ or $\mathsf{Cntr}^u(K_\sigma)$ at least once. Assume the first holds, then there exists $\mathbf{x} \in \mathsf{Cntr}^l(K_\sigma)$ such that $e\mathbf{x}e'$ is feasible. If $e' \subseteq \mathsf{Cntr}_{out}(K_\sigma)$ the proof is conducted in a similar way as the previous case by using the definition of controllability kernel: every point inside the kernel is reachable from any other point in the kernel. □ □

2.4.3 Invariance Kernel

In general, an *invariant set* is a set of points such that for any point in the set, every trajectory starting in such point remains in the set forever and the *invariance kernel* is the largest of such sets. In particular, for SPDI, given a cyclic signature, an *invariant set* is a set of points which keep rotating in the cycle forever and the *invariance kernel* is the largest of such sets. More formally:

Definition 6. *A set K is said to be* invariant *if for any $x \in K$ there exists at least one trajectory starting in it and every trajectory starting in x is viable in K. Given a set K, its largest invariant subset is called the* invariance kernel *of K and is denoted by $\mathsf{Inv}(K_\sigma)$.*

We need some preliminary definitions before showing how to compute the kernel. The *extended ∀-predecessor* of an output edge e of a region R is the set of points in R such that every trajectory segment starting in such point reaches e without traversing any other edge. More formally, let R be a region and e be an edge in $out(R)$, then the *e-extended ∀-predecessor* of I, $\widetilde{\overline{\mathsf{Pre}}}_e(I)$ is defined as:

$$\widetilde{\overline{\mathsf{Pre}}}_e(I) = \{\mathbf{x} \mid \forall\xi\ .\ (\xi(0) = \mathbf{x} \Rightarrow \exists t \geq 0\ .\ (\xi(t) \in I \wedge \mathsf{Sig}(\xi[0,t]) = e))\}.$$

It is easy to see that $\widetilde{\overline{\mathsf{Pre}}}_\sigma(I)$ is a polygonal subset of the plane which can be calculated using the following procedure. First compute $\widetilde{\overline{\mathsf{Pre}}}_{e_i}(I)$ for all $1 \leq i \leq k$ and then apply this operation k times: $\widetilde{\overline{\mathsf{Pre}}}_\sigma(I) = \bigcup_{i=1}^{k} \widetilde{\overline{\mathsf{Pre}}}_{e_i}(I_i)$ with $I_1 = I$, $I_k = \widetilde{\mathsf{Pre}}_{e_k e_1}(I_1)$ and $I_i = \widetilde{\mathsf{Pre}}_{e_i e_{i+1}}(I_{i+1})$, for $2 \leq i \leq k-1$. We compute the invariance kernel of K_σ as follows:

Theorem 6. *If σ is STAY then $\mathsf{Inv}(K_\sigma) = \widetilde{\overline{\mathsf{Pre}}}_\sigma(\widetilde{\mathsf{Pre}}_\sigma(J))$, otherwise $\mathsf{Inv}(K_\sigma) = \emptyset$.* □

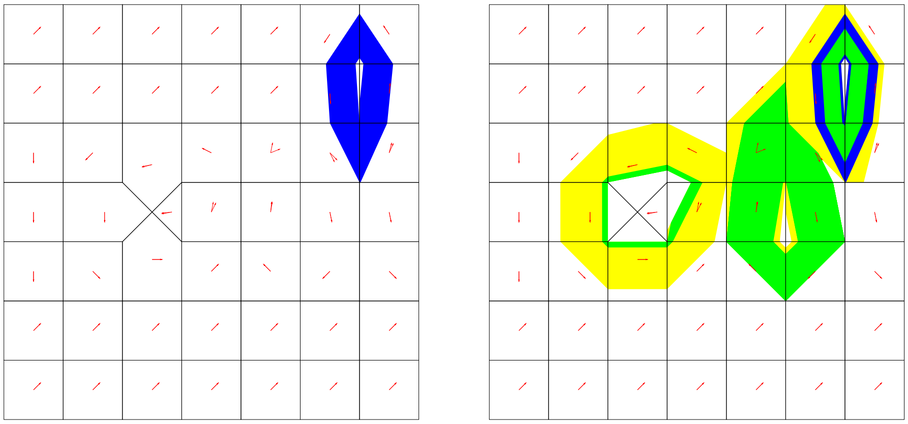
Example 9. *Fig. 4-(a) shows the unique invariance kernels of the SPDI given in Example 1.* ■

An interesting property of invariance kernels is that the limits are included in the invariance kernel, i.e. $[l^*, u^*] \subseteq \mathsf{Inv}(K_\sigma)$. In other words:

Proposition 4. *The set delimited by the polygons defined by the interval $[l^*, u^*]$ is an invariance set of STAY cycles.* □

In [ASY02] it has been proved that for σ a STAY cycle, then (1) $\mathcal{C}(\sigma)$ is invariant and (2) there exists a neighborhood K of $\mathcal{C}(\sigma)$ such that any viable trajectory starting in K converges to $\mathcal{C}(\sigma)$. From this, the definition of invariance kernel and theorem 6 it follows the following result relating controllability and invariance kernels.

Proposition 5. *If $\sigma = e_1 \ldots e_n e_1$ is STAY then $\mathsf{Cntr}(K_\sigma) \subseteq \mathsf{Inv}(K_\sigma)$.* □



(a) (b)

Figure 4: (a) Invariance Kernel; (b) All the Kernels

Example 10. *Fig. 4-(b) shows the viability, controllability and invariance kernels of the SPDI given in Example 1. For any point in the viability kernel of a cycle there exists a trajectory which will converge to its controllability kernel (proposition 2). It is possible to see in the picture that* $\mathsf{Cntr}(\cdot) \subset \mathsf{Inv}(.)$ *(proposition 5). All the above pictures has been obtained with the toolbox SPeeDI*$^{+}$ *[PS06].* ■

In a similar way as for the controllability kernel, we define $\mathsf{Inv}^{l}(K_\sigma)$, $\mathsf{Inv}^{u}(K_\sigma)$, the inner $\mathsf{Inv}_{in}(K_\sigma)$ and outer $\mathsf{Inv}_{out}(K_\sigma)$ of an invariance kernel.

2.5 Semi-Separatrix Curves

In this section we define the notion of *separatrix curves*, which are curves on $\mathbb{R}^2$ dissecting the plane into two mutually non-reachable subsets. We relax the notion of separatrix obtaining *semi-separatrix curves* such that some points in one set may be reachable from the other set, but not vice-versa. We define first the above notions for the plane independently of SPDIs.

Definition 7. *Let $K \subseteq \mathbb{R}^2$. A* separatrix *in K is a closed curve γ partitioning K into three sets K_A, K_B and γ itself, such that $K_A \cap K_B \cap \gamma = \emptyset$, $K = K_A \cup K_B \cup \gamma$ and the following conditions hold:*

1. *For any point $\mathbf{x}_0 \in K_A$ and trajectory ξ, with $\xi(0) = \mathbf{x}_0$, there is no t such that $\xi(t) \in K_B$; and*

2. *For any point $\mathbf{x}_0 \in K_B$ and trajectory ξ, with $\xi(0) = \mathbf{x}_0$, there is no t such that $\xi(t) \in K_A$.*

If only one of the above conditions holds then we say that the curve is a semi-separatrix. *If only condition 1 holds, then we say that K_A is the* inner *of γ (written γ_{in}) and K_B is the* outer *of γ (written γ_{out}). If only condition 2 holds, K_B is the* inner *and K_B is the* outer *of γ.*

Remark: Notice that, as in the case of the controllability kernel, an edge of the SPDI may be split into two by a semi-separatrix — part inside, and part outside. As before, we can split the edge into parts, such that each part is completely inside, or completely outside the semi-separatrix.

The set of all the separatrices of $\mathbb{R}^2$ is denoted by $\mathsf{Sep}(\mathbb{R}^2)$, or simply Sep. The above notions are extended to SPDIs straightforwardly.
Now, let $\sigma = e_1 \ldots e_n e_1$ be a simple cycle, $\angle_{\mathbf{a}_i}^{\mathbf{b}_i}$ $(1 \leq i \leq n)$ be the dynamics of the regions for which e_i is an entry edge and $I = [l, u]$ and interval on edge e_1. Remember that $\mathsf{Succ}_{e_1 e_2}(I) = F(I \cap S) \cap J$, where $F = [a_1 l + b_1, a_2 u + b_2]$. Let $\mathbf{l}$ be the vector corresponding to the point on e_1 with local coordinates l and $\mathbf{l}'$ be the vector corresponding to the point on e_2 with local coordinates $F(l)$ (similarly, we define $\mathbf{u}$ and $\mathbf{u}'$ for $F(u)$). We define first $\overline{\mathsf{Succ}}_{e_1}^{\mathbf{b}_1}(I) = \{\mathbf{x} \mid \mathbf{l}' = \alpha \mathbf{x} + \mathbf{l}, 0 < \alpha < 1\}$ and $\overline{\mathsf{Succ}}_{e_1}^{\mathbf{a}_1}(I) = \{\mathbf{x} \mid \mathbf{u}' = \alpha \mathbf{x} + \mathbf{u}, 0 < \alpha < 1\}$. We extend these definitions in a straight way to any (cyclic) signature $\sigma = e_1 \ldots e_n e_1$, denoting them by $\overline{\mathsf{Succ}}_{\sigma}^{\mathbf{b}}(I)$ and $\overline{\mathsf{Succ}}_{\sigma}^{\mathbf{a}}(I)$, respectively; we can compute them similarly as for $\overline{\mathsf{Pre}}$. Whenever applied to the fix-point $I^* = [l^*, u^*]$, we denote $\overline{\mathsf{Succ}}_{\sigma}^{\mathbf{b}}(I^*)$ and $\overline{\mathsf{Succ}}_{\sigma}^{\mathbf{a}}(I^*)$ by ξ_σ^l and ξ_σ^u respectively. Intuitively, ξ_σ^l (ξ_σ^u) denotes the piece-wise affine closed curve defined by the leftmost (rightmost) fix-point l^* (u^*).
We show now how to identify semi-separatrices for simple cycles.

Theorem 7. *Given an SPDI, let σ be a simple cycle, then the following hold:*

1. *If σ is EXIT-RIGHT then ξ_σ^l is a semi-separatrix curve (filtering trajectories from "left" to "right");*

2. *If σ is EXIT-LEFT then ξ_σ^u is a semi-separatrix curve (filtering trajectories from "right" to "left");*

3. *If σ is STAY, then the two polygons defining the invariance kernel ($\mathsf{Inv}^l(K_\sigma)$ and $\mathsf{Inv}^u(K_\sigma)$), are semi-separatrices.*

Proof.

1. By definition of EXIT-RIGHT, any trajectory is bounded to the left by ξ^l_σ, which is a piece-wise affine closed curve, partitioning $\mathbb{R}^2$ into three disjoint sets: K_B, the "right" part of ξ^l_σ; K_A, the "left" part of ξ^l_σ; and ξ^l_σ itself. By Jordan's theorem, any trajectory may pass from K_B to K_A if and only if it cross ξ^l_σ. However, by definition of EXIT-RIGHT, this is only possible from K_A to K_B but not vice-versa. Hence ξ^l_σ is a semi-separatrix curve.

2. Symmetric to the previous case.

3. Follows directly from the definition of invariance kernel, since any trajectory with initial point in $\mathsf{Inv}(K_\sigma) \cup \mathsf{Inv}_{in}(K_\sigma)$ cannot leave $\mathsf{Inv}(K_\sigma)$. If the trajectory cycles clockwise it cannot traverse $\mathsf{Inv}^l(K_\sigma)$ and if it cycles counter-clockwise it cannot traverse $\mathsf{Inv}^u(K_\sigma)$. In both cases no point on $\mathsf{Inv}_{out}(K_\sigma)$ can be reached. Symmetrically, trajectories starting in $\mathsf{Inv}(K_\sigma) \cup \mathsf{Inv}_{out}(K_\sigma)$ cannot reach any point on $\mathsf{Inv}_{in}(K_\sigma)$. □

□

Remark: In the case of STAY cycles, ξ^l_σ and ξ^u_σ are also semi-separatrices. Notice that in the above result, computing a semi-separatrix depends only on one simple cycle, and the corresponding algorithm is then reduced to find simple cycles in the SPDI and checking whether it is STAY, EXIT-RIGHT or EXIT-LEFT.

Example 11. *Fig. 5 shows all the semi-separatrices of the SPDI given in Example 1. The small arrows traversing the semi-separatrices show the inner and outer of each semi-separatrix: a trajectory may traverse the semi-separatrix following the direction of the arrow, but not vice-versa.* ■

The following two results relate feasible signatures and semi-separatrices.

Proposition 6. *If, for some semi-separatrix γ, $e \in \gamma_{in}$ and $e' \in \gamma_{out}$, then the signature ee' is not feasible.* □

Proof. Directly from the definition of semi-separatrix. □ □

Proposition 7. *If, for some semi-separatrix γ, and signature σ (of at least length 2), then, if head(σ) $\in \gamma_{in}$ and last(σ) $\in \gamma_{out}$, σ is not feasible.*

Proof. The proof proceeds by induction on sequence σ. The base case, when σ is of length 2, reduces to proposition 6. Now, assuming that the proposition is true for signatures of length n, we are required to prove that it is also true for signatures of length $n + 1$. Consider the signature $\sigma' = ee'\sigma e''$, with $e \in \gamma_{in}$ and $e'' \in \gamma_{out}$. Clearly, either $e' \in \gamma_{in}$ or $e' \in \gamma_{out}$.

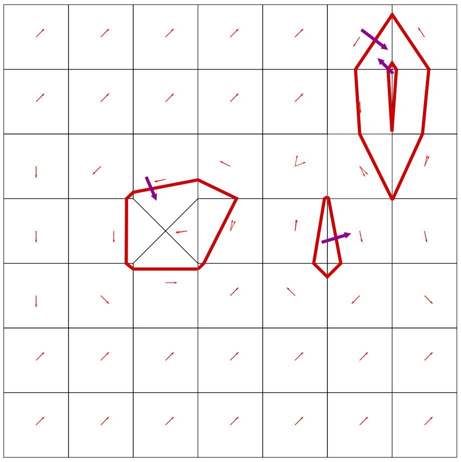


Figure 5: Semi-separatrices

Case 1: $e' \in \gamma_{in}$. The signature $e'\sigma e''$ satisfies the conditions and is of length n. Therefore, the inductive property applies, and we can conclude that $e'\sigma e''$ is not feasible. However, since any extension of an unfeasible signature is itself unfeasible, it follows that σ' is not feasible.

Case 2: $e' \in \gamma_{out}$. The signature ee' is unfeasible by proposition 6. Therefore, being an extension of ee', σ' is also unfeasible (proposition 1). □

□

3 State-Space Reduction Using Semi-Separatrices

Semi-separatrices partition the state space into two parts[3] – once one crosses such a border, all states outside the region can be ignored. We present a technique, which, given an SPDI and a reachability question, enables us to discard portions of the state space based on this information. The approach is based on identifying *inert* states (edges in the SPDI) which cannot play a role in the reachability analysis.

Definition 8. *Given an SPDI $\mathcal{S}$, a set of semi-separatrices $\Gamma \subseteq \mathsf{Sep}$, a source edge $e0$ and a destination edge $e1$, an edge e is said to be* inert *if it lies outside a semi-separatrix inside which lies $e0$, or it lies inside a semi-separatrix outside which lies $e1$:*

[3] We don't consider the semi-separatrix itself.

$$\begin{array}{rcl} \mathit{inert}^{\Gamma}_{e0\to e1} & = & \{e : \mathcal{E} \mid \exists \gamma \in \Gamma \cdot e0 \in \gamma_{in} \wedge e \in \gamma_{out}\} \\ & \cup & \{e : \mathcal{E} \mid \exists \gamma \in \Gamma \cdot e1 \in \gamma_{out} \wedge e \in \gamma_{in}\} \blacksquare \end{array}$$

We can prove that these inert edges can never appear in a feasible signature:

Lemma 8. *Given an SPDI $\mathcal{S}$, a set of semi-separatrices Γ, a source edge $e0$ and a destination edge $e1$, and a feasible signature $e0\sigma e1$ in $\mathcal{S}$. No inert edge from $\mathit{inert}^{\Gamma}_{e0\to e1}$ may appear in $e0\sigma e1$.*

Proof. From the definition of inert states, it follows that either both $e0$ and $e1$ are inert, or neither is. If both are inert, then for some γ, $e0 \in \gamma_{in}$ and $e1 \in \gamma_{out}$. But if this were so, then $e0\sigma e1$ is unfeasible by proposition 7. We can thus consider only inert edges in σ.
Let e be an inert edge appearing in σ. Therefore, $e0\sigma e1 = e0\sigma_1 e\sigma_2 e1$. By definition of inert edges, e can either be inert because (i) it lies outside a semi-separatrix inside which lies $e0$, or (ii) it lies inside a semi-separatrix outside which lies $e1$.

Case 1: Let $\gamma \in \Gamma$ be a semi-separatrix such that $e0 \in \gamma_{in}$ and $e \in \gamma_{out}$. But by proposition 7, $e0\sigma_1 e$ is not feasible. Hence, neither is $e0\sigma_1 e\sigma_2 e1$.

Case 2: Let $\gamma \in \Gamma$ be a semi-separatrix such that $e \in \gamma_{in}$ and $e1 \in \gamma_{out}$. By proposition 7, $e\sigma_2 e1$ is not feasible, and hence, neither is $e0\sigma_1 e\sigma_2 e1$.

It thus follows that $e0\sigma e1$ is not feasible. □

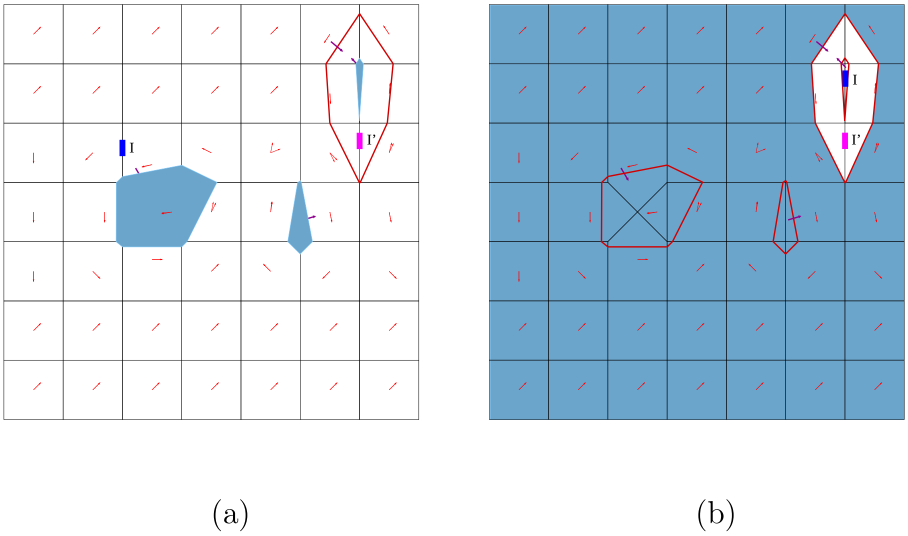
Given an SPDI, we can reduce the state space by discarding inert edges.

Definition 9. *Given an SPDI $\mathcal{S}$, a set of semi-separatrices Γ, a source edge $e0$ and a destination edge $e1$, we define the reduced SPDI $\mathcal{S}^{\Gamma}_{e0\to e1}$ to be the same as $\mathcal{S}$ but without the inert edges.* ■

Clearly, the resulting SPDI is smaller than the original one.

Proposition 8. *For any SPDI $\mathcal{S}$, a set of semi-separatrices Γ, and edges $e0$ and $e1$, $\mathcal{S}$ does not have less edges than $\mathcal{S}^{\Gamma}_{e0\to e1}$.* □

Example 12. *The shaded (light blue) areas of Fig. 6 (a) and (b) are the subsets of the SPDI (edges of the reachability graph) eliminated by the reduction presented in this section, when answering the question: Is interval I' reachable from I?* ■



(a) (b)

Figure 6: Reduction using Semi-separatrices

Finally, we prove that checking reachability on the reduced SPDI is equivalent to checking reachability on the original SPDI:

Theorem 9. *Given an SPDI $\mathcal{S}$, a set of semi-separatrices Γ, and edges $e0$ and $e1$, then, $e1$ is reachable from $e0$ in $\mathcal{S}$ if and only if $e1$ is reachable from $e0$ in $\mathcal{S}^{\Gamma}_{e0\rightarrow e1}$.*

Proof. The proof is split into two parts: that reachability in the reduced SPDI implies reachability in the original automaton (soundness) and vice-versa (completeness).

Soundness: Assume that $e1$ is reachable from $e0$ in $\mathcal{S}^{\Gamma}_{e0\rightarrow e1}$. Then, there must exist a feasible signature σ in $\mathcal{S}^{\Gamma}_{e0\rightarrow e1}$ which starts on $e0$ and ends at $e1$. Since every SPDI edge in $\mathcal{S}^{\Gamma}_{e0\rightarrow e1}$ is also in $\mathcal{S}$, and the dynamics of the two systems are identical, it follows that σ is also a feasible path in $\mathcal{S}$. Therefore, $e1$ is also reachable from $e0$ in $\mathcal{S}$.

Completeness: Now assume that $e1$ is reachable from $e0$ in $\mathcal{S}$. By definition of reachability, there exists a feasible signature $e0\sigma e1$ in $\mathcal{S}$. By proposition 8, no inert edge may appear in $e0\sigma e1$. Therefore, $e0\sigma e1$ is also a feasible signature in $\mathcal{S}^{\Gamma}_{e0\rightarrow e1}$, which in turn implies that $e1$ is reachable from $e0$ in $\mathcal{S}_{e0\rightarrow e1}$. □

□

We have shown, that once semi-separatrices are identified, given a reachability question, we can reduce the size of the SPDI to be verified. This enables us to verify SPDIs much more efficiently. It is important to note that model-checking an SPDI requires identification of simple loops, which means that the calculation of the semi-separatrices is not more expensive than the initial pass of the model-checking algorithm. Furthermore, we can perform this analysis only once for an SPDI and store the information to be used in any reachability analysis on that SPDI. Reduction, however, can only be applied once we know the source and destination states.

4 State-Space Reduction Using Kernels

4.1 State-space reduction using kernels

We have already shown that any invariant set, is essentially a pair of semi-separatices. In particular, the invariance kernel is a largest invariant set for a particular loop, we can use the results presented in section 3 to abstract an SPDI by using invariance kernels. We now turn our attention to state space reduction using controllability kernels:

Definition 10. *Given an SPDI $\mathcal{S}$, a loop σ, a source edge $e0$ and a destination edge $e1$, an edge e is said to be* redundant *if it lies on the opposite side of a controllability kernel as both $e0$ and $e1$:*

$$\begin{array}{rcl} \mathit{redundant}^{\sigma}_{e0\to e1} & = & \{e : \mathcal{E} \mid \exists e0,\ e1 \in \mathsf{Cntr}_{in}(\sigma) \cup \mathsf{Cntr}(\sigma) \wedge e \in \mathsf{Cntr}_{out}(\sigma)\} \\ & \cup & \{e : \mathcal{E} \mid \exists e0,\ e1 \in \mathsf{Cntr}_{out}(\sigma) \cup \mathsf{Cntr}(\sigma) \wedge e \in \mathsf{Cntr}_{in}(\sigma)\} \ \blacksquare \end{array}$$

We can prove that we can do without these edges to check feasibility:

Lemma 10. *Given an SPDI $\mathcal{S}$, a loop σ, a source edge $e0$, a destination edge $e1$, and a feasible signature $e0\sigma e1$ then there exists a feasible signature $e0\sigma' e1$ such that σ' contains no redundant edge from $\mathit{redundant}^{\sigma}_{e0\to e1}$.*

Proof. Let $e0\sigma e1$ be a feasible signature which contains some redundant edge from the set $\text{redundant}^{\sigma}_{e0\to e1}$. Without loss of generality, we assume that $e0,\ e1 \in \mathsf{Cntr}_{out}(\sigma) \cup \mathsf{Cntr}(\sigma)$. Let $f0$ and $f1$ be, respectively, the first and last redundant edges in σ. By definition of redundant edges, it follows that $f0,\ f1 \in \mathsf{Cntr}_{in}(\sigma)$. The path we are following is thus:

$$e0\sigma_1 f0\sigma_2 f1\sigma_3 e1$$

Since $f0$ ($f1$) is the first (last) redundant edge, it follows that the last element of σ_1 (the first element of σ_3) is inside the controllability kernel. Using proposition 3, it follows that there exists a point p on the controllability kernel reachable from the last element of σ_1 (a point q on the controllability kernel from which the first element of σ_3 is reachable). Since all points on the controllability kernel are mutually reachable, it follows that q is reachable from p along some discrete path σ_2' completely within the kernel. We have thus obtained a shorter discrete path $e0\sigma_1\sigma_2'\sigma_3 e1$ which is feasible and which contains no redundant edges. □ □

Given an SPDI, we can reduce the state space by discarding redundant edges.

Definition 11. *Given an SPDI $\mathcal{S}$, a loop σ, a source edge* e0 *and a destination edge* e1*, we define the reduced SPDI $\mathcal{S}^{\sigma}_{e0\to e1}$ to be the same as $\mathcal{S}$ but without redundant edges.* ■

Clearly, the resulting SPDI is smaller than the original one.

Proposition 9. *For any SPDI $\mathcal{S}$, a loop σ, a source edge* e0 *and a destination edge* e1*, $\mathcal{S}$ does not have less edges than $\mathcal{S}^{\sigma}_{e0\to e1}$.* □

Finally, we prove that checking reachability on the reduced SPDI is equivalent to checking reachability on the original SPDI:

Theorem 11. *Given an SPDI $\mathcal{S}$, with a set of loops σ, a source edge* e0 *and a destination edge* e1*, then,* e1 *is reachable from* e0 *in $\mathcal{S}$ if and only if* e1 *is reachable from* e0 *in $\mathcal{S}^{\sigma}_{e0\to e1}$.*

Proof. The theorem follows immediately from proposition 10. □ □

Given a loop which has a controllability kernel, we can thus reduce the state space to explore. In practice, we apply this state space reduction for each controllability kernel in the SPDI. Once a loop in the SPDI is identified, it is straightforward to apply the reduction algorithm.

4.2 Immediate answers to reachability questions

By definition of the controllability kernel, any two points inside it are mutually reachable. This can be used to answer certain reachability questions simply by inspecting the controllability kernel: if both the source and destination edge lie (possibly partially) within the same controllability kernel, then, there exists a trajectory from the source to the destination edge.

Proposition 10. *Given a source edge e_{src} and a destination edge e_{dst}, if for some loop σ, $e_{src} \cap \mathsf{Cntr}(K_\sigma) \neq \emptyset$ and $e_{dst} \cap \mathsf{Cntr}(K_\sigma) \neq \emptyset$, then e_{dst} is reachable from e_{src}.* □

Furthermore, proposition 2 tells us that any point in the viability kernel of a loop can eventually reach the controllability kernel of the same loop. This allows us to relax the condition about the source edge to just check whether it (partially) lies within the viability kernel. Since the controllability kernel always lies within the viability kernel of the same loop, this is a generalization of the first result.

Proposition 11. *Given a source edge e_{src} and a destination edge e_{dst}, if for some loop σ, $e_{src} \cap \mathsf{Viab}(K_\sigma) \neq \emptyset$ and $e_{dst} \cap \mathsf{Cntr}(K_\sigma) \neq \emptyset$, then e_{dst} is reachable from e_{src}.* □

Finally, we note that the union of two non-disjoint controllability sets is itself a controllability set. This means that we can extend the result to work for a collection of loops whose controllability kernels form a strongly connected set. To state this result, we will require some additional machinery.

Definition 12. *We extend viability and controllability kernels for a set of loops Σ by taking the union of the kernels of the individual loops:*

$$\begin{aligned} \mathsf{Viab}(K_\Sigma) &= \bigcup_{\sigma \in \Sigma} \mathsf{Viab}(K_\sigma) \\ \mathsf{Cntr}(K_\Sigma) &= \bigcup_{\sigma \in \Sigma} \mathsf{Cntr}(K_\sigma) \blacksquare \end{aligned}$$

Definition 13. *Two loops σ and σ' are said to be compatible ($\sigma \leftrightsquigarrow \sigma'$) if their controllability kernels overlap:*

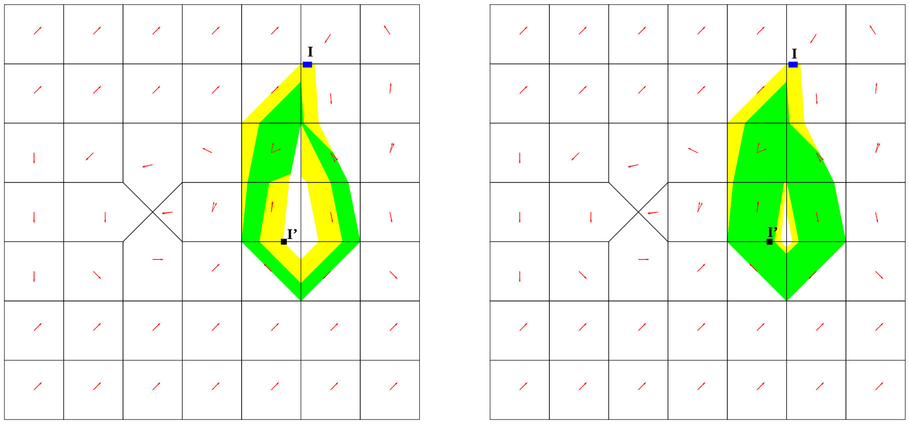
$$\sigma \leftrightsquigarrow \sigma' \Leftrightarrow \mathsf{Cntr}(K_\sigma) \cap \mathsf{Cntr}(K'_\sigma) \neq \emptyset$$

We extend the notion of compatibility to a set of loops Σ to mean that all loops in the set are transitively compatible:

$$\forall \sigma,\ \sigma' \in \Sigma \ \cdot \ \sigma \leftrightsquigarrow^* \sigma'$$

■

Theorem 12. *Given a source edge e_{src} and a destination edge e_{dst}, if for some compatible set of loops Σ, $e_{src} \cap \mathsf{Viab}(K_\Sigma) \neq \emptyset$ and $e_{dst} \cap \mathsf{Cntr}(K_\Sigma) \neq \emptyset$, then e_{dst} is reachable from e_{src}.*



(a) (b)

Figure 7: Answering Reachability using Kernels

Proof. The proof of the theorem follows almost immediately from the definition of the controllability kernel, and proposition 2. □ □

We note that this theorem is a generalization of the previous two propositions.

Example 13. *Fig. 7-(a) shows a viability and a controllability kernel of a cycle and two intervals I and I'. The reachability question, is I' reachable from I?, cannot be answered immediately in this case. Fig. 7-(b) shows overlapping of the viability and controllability kernels depicted in Fig. 7-(a) with the kernels of an inner cycle. I' is shown to lie in a compatible controllability kernel, thus by theorem 12, I' is reachable from I (the positive answer is given without the need of performing the reachability analysis).* ■

The next theorem provides an immediate answer to edges lying inside and outside invariance kernels. The proof follows directly from the definition of invariance kernels.

Theorem 13. *If one of the following conditions holds, then then e_{dst} is not reachable from e_{src}:*

1. *Source edge $e_{src} \in \mathsf{Inv}_{in}(K_\sigma)$ and destination edge $e_{dst} \in \mathsf{Inv}(K_\sigma) \cup \mathsf{Inv}_{out}(K_\sigma)$*
2. *Source edge $e_{src} \in \mathsf{Inv}(K_\sigma) \cup \mathsf{Inv}_{out}(K_\sigma)$ and destination edge $e_{dst} \in \mathsf{Inv}_{in}(K_\sigma)$* □

We note that, since an invariance kernel induces a pair of semi-separatrices, this theorem is a specialization of of the reduction using semi-separatrix information.

In practice, we propose to use these theorems to enable answering certain reachability questions without having to explore the complete state space. It can also be used to reduce reachability questions to (possibly) simpler ones by trying to reach a viability kernel rather than a particular edge (in the case of theorem 12). As in the case of semi-separatrices, a preliminary analysis of an SPDI can be done to store all kernels, which information is used in all subsequent reachability queries. By combining this technique with the semi-separatrix reduction technique we envisage substantial gains.

5 Concluding Remarks

We have hereby introduced the concept of semi-separatrices for polygonal hybrid systems, and presented non-iterative algorithms to calculate them.

Using semi-separatrices, and kernels in SPDI phase-portraits introduced in [ASY02] and in [Sch04], we presented techniques to improve reachability analysis on SPDIs. In all cases, the techniques require the identification and analysis of loops in the SPDI. When multiple reachability questions are to be asked about the same SPDI, this information can be gathered and stored to avoid repeated analysis. We note that most of this information is still required when performing reachability analysis, and thus no extra work is required to perform the optimization presented in this paper. The results presented in this paper all depend on checking whether an edge lies within a given polygon. This can be efficiently checked using standard geometrical techniques frequently used in computer graphics such as using the odd-parity test [FvDFH96].

In certain cases, using kernel information, we can answer reachability questions using the information gathered without any further analysis. In other cases, we use semi-separatrices and controllability kernels to reduce the size of the SPDI under analysis.

Our work is obviously restricted to planar systems, which enables us to compute these kernels exactly. In higher dimensions and hybrid systems with higher complexity, calculation of kernels is not computable. Other related work is thus based on calculations of approximations of these kernels (e.g., [ALQ$^+$01b, ALQ$^+$01a, SP02]). We are not aware of any work using kernels and semi-separatrices to reduce the state-space of the reachability graph as presented in this paper.

We have built a toolset SPeeDI [APSY02] for the analysis of SPDIs. We have recently extended this toolset to SPeeDI$^+$ [PS06] which calculates kernels of SPDIs. We are currently exploring the implementation of the optimizations presented in this paper to improve the efficiency of SPeeDI$^+$. We are also investigating other applications of these kernels in the model-checking of SPDIs.

References

[AD94] R. Alur and D.L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126:183–235, 1994.

[ALQ$^+$01a] J.-P. Aubin, J. Lygeros, M. Quincampoix, S. Sastry, and N. Seube. Towards a viability theory for hybrid systems. In *European Control Conference*, 2001.

[ALQ$^+$01b] J.-P. Aubin, J. Lygeros, M. Quincampoix, S. Sastry, and N. Seube. Viability and invariance kernels of impulse differential inclusions. In *Conference on Decision and Control*, volume 40 of *IEEE*, pages 340–345, December 2001.

[APSY02] E. Asarin, G. Pace, G. Schneider, and S. Yovine. SPeeDI: a verification tool for polygonal hybrid systems. In *CAV'2002*, volume 2404 of *LNCS*, pages 354–358, Copenhagen, Denmark, July 2002. Springer-Verlag.

[ASY01] E. Asarin, G. Schneider, and S. Yovine. On the decidability of the reachability problem for planar differential inclusions. In *HSCC'2001*, number 2034 in LNCS, pages 89–104, Rome, Italy, 2001. Springer-Verlag.

[ASY02] E. Asarin, G. Schneider, and S. Yovine. Towards computing phase portraits of polygonal differential inclusions. In *HSCC'02*, pages 49–61. LNCS 2289, Springer, 2002.

[Aub01] J.-P. Aubin. The substratum of impulse and hybrid control systems. In *HSCC'01*, volume 2034 of *LNCS*, pages 105–118. Springer, 2001.

[DV95] A. Deshpande and P. Varaiya. Viable control of hybrid systems. In *Hybrid Systems II*, number 999 in LNCS, pages 128–147, 1995.

[FvDFH96] James D. Foley, Andries van Dam, Steven K. Feiner, and John F. Hughes. *Computer graphics (2nd ed. in C): principles and practice*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1996.

[Hen79] Michael Henle. *A combinatorial introduction to topology.* Dover publications, Inc., 1979.

[HKPV95] T.A. Henzinger, P.W. Kopke, A. Puri, and P. Varaiya. What's decidable about hybrid automata? In *STOC'95*, pages 373–382. ACM Press, 1995.

[KdB01] P. Kowalczyk and M. di Bernardo. On a novel class of bifurcations in hybrid dynamical systems. In *HSCC'01*, number 2034 in LNCS, pages 361–374. Springer, 2001.

[LPY01] G. Lafferriere, G. Pappas, and S. Yovine. Symbolic reachability computation of families of linear vector fields. *Journal of Symbolic Computation*, 32(3):231–253, September 2001.

[MP93] O. Maler and A. Pnueli. Reachability analysis of planar multi-linear systems. In *CAV'93*, pages 194–209. LNCS 697, Springer Verlag, July 1993.

[MS00] A. Matveev and A. Savkin. *Qualitative theory of hybrid dynamical systems*. Birkhäuser Boston, 2000.

[PS06] G. Pace and G. Schneider. Computation and visualization of phase portraits for model checking SPDI. 2006. Submitted.

[Sch04] G. Schneider. Computing invariance kernels of polygonal hybrid systems. *Nordic Journal of Computing*, 11(2):194–210, 2004.

[SJSL00] S. Simić, K. Johansson, S. Sastry, and J. Lygeros. Towards a geometric theory of hybrid systems. In *HSCC'00*, number 1790 in LNCS, pages 421–436. Springer, 2000.

[SP02] P. Saint-Pierre. Hybrid kernels and capture basins for impulse constrained systems. In *HSCC'02*, volume 2289 of *LNCS*. Springer-Verlag, 2002.