ABSTRACT
We analyze the properties of differentiable trajectories subject to a constant differential inclusion which constrains the first derivative to belong to a given convex polyhedron. We present the first exact algorithm that computes the set of points from which there is a trajectory that reaches a given polyhedron while avoiding another (possibly non-convex) polyhedron. We discuss the connection with (Linear) Hybrid Automata and in particular the relationship with the classical algorithm for reachability analysis for Linear Hybrid Automata.

1. INTRODUCTION
Hybrid Automata are a mathematical abstraction of systems that feature both discrete and continuous dynamics. Linear Hybrid Automata (LHAs) [2] were introduced as a computationally tractable model of hybrid systems that still allows for non-trivial dynamics. In particular, LHAs can approximate complex dynamics up to an arbitrary precision [10].

In an LHA, discrete dynamics is represented by a finite set of control modes called locations, while the continuous dynamics is ensured by a finite set of real-valued variables. In each discrete location, the continuous dynamics is constrained by a differential inclusion of the type \( \dot{x} \in F \), where \( \dot{x} \) is the vector of the time-derivatives of all the variables in the system, and \( F \subseteq \mathbb{R}^n \) is a convex polyhedron. The main decision problem that was considered for LHAs is reachability, i.e., given two system configurations, say an initial state and an error state, establish whether there is a system behavior that leads from the first to the second. A more complex task consists in verifying whether a given LHA can be modified (i.e., controlled) in such a way that a given error configuration (or region) is not reached by any behavior. This problem can be called safety control and is analogous to a game with a safety objective. Both problems require an algorithm for the following sub-problem, which applies to a single discrete location: given a region \( G \) (for goal) and a region \( A \) (for avoid) of system configurations, find the set of points from which there is a trajectory that reaches \( G \) while avoiding \( A \) at all times. We denote this set by \( RWA(G,A) \) for reach while avoiding. In reachability problems, the goal region \( G \) can be thought of as error states, and the avoidance region \( A \) is the complement of the invariant of the automaton, which is the set of configurations that make physical sense for the system. Hence, \( RWA(G,A) \) is the set of states that reach an error state while remaining in the invariant. In a safety control problem, the goal region \( G \) is taken to be a set of uncontrollable states (such as, states outside the safe region) and \( A \) is a set of controllable states (included in the invariant). Then, \( RWA(G,A) \) identifies the region in which the environment can reach an error state while avoiding the good, controllable states.

The \( RWA \) operator is recognized as a central tool in the analysis of various kinds of hybrid systems: it corresponds to the Reach operator in Tomlin et al. [12] and Unavoid_Pre in Balluchi et al. [4]; it was also used in the synthesis of controllers for reachability objectives [8].

Computing reach-while-avoiding. Computing of \( RWA(G,A) \) is simple when \( A \) is co-convex, corresponding to the case of reachability analysis for LHAs with convex invariants. In that case, \( RWA \) can be expressed in the first-order theory of reals and computed using a constant number of basic polyhedra operations.

When \( A \) is not co-convex, one may adapt the procedure that is presented in one of the early papers on LHAs, in the context of reachability analysis in presence of non-convex invariants [2]. The idea of the algorithm is simple: consider a partition of the non-convex invariant \( I \) into a finite set of convex polyhedra \( P_1, \ldots, P_n \); then, split the location with invariant \( I \) into \( n \) different locations, each with convex invariant \( P_i \); finally, connect these new locations with virtual transitions corresponding to the boundaries between two adjacent convex polyhedra \( P_i, P_j \).

The problem with this approach is that the discrete transitions that model the crossing from one convex polyhedron to an adjacent one do not preserve the differentiability of the trajectories. In other words, there are trajectories in the modified system that do not correspond to any trajectory in the original system. Consider for example the situation depicted in Figure 1. Assume that the invariant for the current location is \( P \cup Q \cup G \) and the goal is to reach \( G \). Dashed lines identify topologically open sides of polyhedra. The flow constraint \( F \) is also depicted in the figure: it allows trajectories to
move in a range of directions going from straight right to straight up, and it forbids stopping (i.e., it does not include the origin).

The above procedure splits the invariant into three convex polyhedra, and then performs a backward reachability analysis which starts from the goal $G$ and progressively enlarges the set of "good" states $W$ by including the states that can reach $W$ while remaining in one of the convex parts of the invariant.

In our example, the points in the line segment $Q$ can reach the target by moving straight to the right, while remaining in one convex part of the invariant. Hence, in the first iteration the set $Q$ is added to the set of good states $W$. The points in the line segment $P$ can reach the extreme point of $Q$ by moving straight up. Hence, in the second iteration the above procedure puts $P$ in $W$. On the other hand, no differentiable trajectory can start in a point of $P$ and reach $G$ while remaining in $P \cup Q \cup G$. In other words, the classical algorithm for reachability analysis of LHAs computes the set of points that can reach-while-avoiding via a trajectory that can take a finite number of sharp turns, i.e., a trajectory that is differentiable almost everywhere.

By rotating the polyhedra in Figure 1 (including the flow constraint $F$) by $45^\circ$, it becomes apparent that the issue is also present with rectangular flow constraints. However, Rectangular Hybrid Automata and Games [11] do not exhibit the above issue, due to the presence of multiple restrictions, such as the fact that guards and invariants are convex and topologically closed.

In this paper, we present an exact algorithm for computing $RWA(G, A)$ for general polyhedra $G$ and $A$, assuming that trajectories are differentiable everywhere.

The rest of the paper is organized as follows. Section 2 is devoted to preliminary definitions, including the problem statement. In Section 3 we recall the previous attempts at computing $RWA$ and remark that they only work for trajectories that are almost everywhere differentiable. We also lay the basis for our algorithm, by introducing an operator (called Cross) that contains the points that can move in a differentiable fashion from a given convex polyhedron $P$ to another one $P'$ and spend a positive amount of time in the latter. In Section 4 we present a series of steps that lead from Cross (which deals with arbitrary differentiable trajectories) to a computationally simpler operator (called ClosCross) that only reasons about straight-line trajectories. Then, in Section 5 we show how the latter operator can be computed using basic operations on polyhedra. Section 6 argues that a finite number of repeated applications of Cross (plus a preliminary step) captures exactly $RWA$. Finally, we provide some conclusions in Section 7.

2. DEFINITIONS

Let $\mathbb{R}$ (respectively, $\mathbb{R}_{\geq 0}$) denote the set of real numbers (resp., non-negative real numbers). Throughout the paper we consider a fixed ambient space $\mathbb{R}^n$. A convex polyhedron is a subset of $\mathbb{R}^n$ that is the intersection of a finite number of open and closed half-spaces. A polyhedron is a subset of $\mathbb{R}^n$ that is the union of a finite number of convex polyhedra. For a general (i.e., not necessarily convex) polyhedron $G \subseteq \mathbb{R}^n$, we denote by $cl(G)$ its topological closure, by $\bar{G}$ its complement, and by $[G] \subseteq 2^{\mathbb{R}^n}$ its representation as a finite set of convex polyhedra. We assume w.l.o.g. that $[G]$ contains mutually disjoint convex polyhedra, called patches of $G$.

Let $C \subseteq [\mathbb{R}_{\geq 0} \rightarrow \mathbb{R}^n]$ be a class of functions from the time domain to our ambient space. Given a convex polyhedron $F$, called the flow constraint, an $(F,C)$-trajectory is a function $f \in C$ such that $\dot{f}(t) \in F$ for all $t \geq 0$ such that $f$ is differentiable in $t$. Given a point $x \in \mathbb{R}^n$, let $Adm^F_x(x)$ (for admissible) denote the set of $(F,C)$-trajectories $f$ starting from $x$ (i.e., such that $f(0) = x$). We henceforth consider two classes of functions: the class $C_d$ of functions that are continuous and differentiable almost everywhere, and the class $C_{ae}$ of functions that are continuous everywhere and differentiable almost everywhere (i.e., always except for a finite set of time points).

Given two disjoint polyhedra $G$ (for goal) and $A$ (for avoid), we denote by $RWA^F(G, A)$ (for reach while avoiding) the set of points from which there is an $(F,C)$-trajectory that reaches $G$ while avoiding $A$. Formally, we have:

$$RWA^F(G, A) = \{ x \in \mathbb{R}^n \mid \exists f \in Adm^F_x(x), \delta_f \geq 0 : f(\delta_f) \in G \land 0 \leq \delta < \delta_f : f(\delta) \notin A \}.$$

For every $x \in RWA^F(G, A)$, any pair $(f, \delta_f)$ satisfying the condition in the definition of $RWA^F$ will be called a witness for $x$. Notice that

$$RWA^F(G_1 \cup G_2, A) = RWA^F(G_1, A) \cup RWA^F(G_2, A),$$

whereas $RWA^C_F$ does not distribute over unions in the second argument (see [?]). Therefore, in the following we can assume, w.l.o.g., that the goal $G$ is a convex polyhedron.

3. TRACKING DIFFERENTIABLE TRAJECTORIES

Starting from this section, we consider a fixed flow constraint $F$, and we omit the $F$ parameter from all notations.

3.1 The Previous Algorithm

Let us briefly recall the previous approach to the problem, which can be used to compute $RWA$, assuming that trajectories are differentiable everywhere except for a finite set of time points.

Given two convex polyhedra $P, P'$, let $Reach(P, P')$ be the set of points in $P$ that can reach $P'$ via a trajectory that remains within $P \cup P'$ at all times (until $P'$ is reached).
Formally, \( \text{Reach}(P, P') = \{ x \in P \mid \exists f \in \text{Adm}^c(x), \delta \geq 0 : f(\delta) \in P' \land \forall \delta' \in (0, \delta) : f(\delta') \in P \cup P' \} \).

It can be shown that \( \text{Reach}(P, P') \) is a convex polyhedron which can be computed from \( P, P' \), and \( P \) using basic polyhedra operations \([5, 7]\). Then, Theorem 1 shows how \( \text{RWA} \) can be computed by iterative application of \( \text{Reach} \).

**Theorem 1.** \([5, 7]\) For all polyhedra \( G, A, \) and \( W \), let \( \tau_{\text{ua}}(G, A, W) = G \cup \bigcup_{P \in [G]} \bigcup_{P' \in [W]} \text{Reach}(P, P') \).

We have \( \text{RWA}^{\text{ua}}(G, A) = \mu W \cdot \tau_{\text{ua}}(G, A, W) \), where \( \mu W \) denotes the least fixed point operator. Moreover, the fixed point is reached within a finite number of iterations.

By Knaster-Tarski fixed point theorem, the fixed point equation in Theorem 1 suggests the semi-algorithm consisting in repeated applications of \( \tau_{\text{ua}}(G, A, W) \), starting from \( W = \emptyset \), i.e.: \( W_0 = \emptyset \) and \( W_{i+1} = \tau_{\text{ua}}(G, A, W_i) \) for all \( i \geq 0 \). Theorem 1 states that there exists \( k \geq 0 \) such that \( W_k = W_{k+1} = \text{RWA}^{\text{ua}}(G, A) \).

The \( \text{Reach} \) and \( \tau_{\text{ua}} \) operators, together with Theorem 1, represent a reformulation of the original algorithm for reachability analysis of LHAs under convex invariants, which was expressed in terms of locations of a hybrid automaton. Notice that both ourselves (in \([5]\), later corrected by \([7]\)) and Alur et al. (in \([1, 2]\)) have claimed that \( \tau_{\text{ua}} \) (or very similar variations thereof) can be used to compute \( \text{RWA}^{\text{ua}} \). Those claims are incorrect, as shown in the Introduction and again below. In the rest of the paper we show that significant new developments are required to correctly compute \( \text{RWA}^{\text{ua}} \).

### 3.2 Differentiable Trajectories

Consider again the example in Figure 1, and let \( A = A_1 \cup A_2 \). It holds \( \text{Reach}(Q, G) = Q \) and \( \text{Reach}(P, Q) = P \). On the other hand, when considering differentiable trajectories it holds \( \text{RWA}^{\text{ua}}(G, A) = G \cup Q \). The points in \( P \) do not belong to \( \text{RWA}^{\text{ua}}(G, A) \) because no differentiable trajectory can start from \( P \) and turn into \( Q \) without hitting either \( A_1 \) or \( A_2 \).

An obvious first step consists in modifying the definition of \( \text{Reach} \) by replacing \( \text{Adm}^C \) with \( \text{Adm}^{\text{ua}} \). However, this replacement is not sufficient to solve the problem with the example in Figure 1: it would still hold \( \text{Reach}(P, Q) = P \), because the points in \( P \) can reach \( Q \) along a straight-line trajectory, which is both in \( C_{\text{ua}} \) and in \( C_\circ \).

Then, we notice that all trajectories going from \( P \) to \( Q \) lie within \( P \) at all times, except for the final point, which belongs to \( Q \). Hence, we modify the definition of \( \text{Reach}(P, P') \) by requiring not only that there exists a (differentiable) trajectory from \( P \) to \( P' \) contained in \( P \cup P' \), but also that this trajectory spends a positive amount of time in \( P' \):

\[ \text{Reach}'(P, P') = \{ x \in P \mid \exists f \in \text{Adm}^C(x), 0 \leq \delta_1 < \delta_2 : \forall \delta \in (0, \delta_1) : f(\delta) \in P \cup P' \land \forall \delta \in (\delta_1, \delta_2) : f(\delta) \in P' \} \].

Unfortunately, \( \text{Reach}' \) still suffers from a shortcoming. Consider again the example in Figure 1, but this time let the avoidance region be \( A = A_1 \). Notice that the status of the immediate neighborhood of \( P \) is identical to the previous case: \( Q \) is still a “good” neighbor (w.r.t. reaching \( G \) while avoiding \( A \)) and \( A_1 \) is still a “bad” neighbor. However, we have \( P \subseteq \text{RWA}^{\text{ua}}(G, A) \), because a differentiable trajectory can start from \( P \), pass instantaneously through the left vertex of \( Q \), then curve into \( A_2 \) and finally reach \( G \). The fact that \( P \) is a set of good points is essentially due to \( A_2 \), which is not an immediate neighbor of \( P \) (in our terminology, it is a weak neighbor, since \( cl(P) \cap cl(A_2) \neq \emptyset \)).

Therefore, we realize that \( \text{Reach}' \) cannot solve this example because it is constrained to consider pairs of adjacent convex polyhedra. In particular, it holds \( \text{Reach}'(P, A_2) = \emptyset \) because \( P \) and \( A_2 \) are not adjacent, and \( \text{Reach}'(P, Q) = \emptyset \) because differentiable trajectories cannot start from \( P \) and spend a positive amount of time in \( Q \) while remaining in \( P \cup Q \).

Guided by this example, we devise a third version of \( \text{Reach} \), called \( \text{Cross} \), which carries three arguments: \( \text{Cross}(P, P, P') \) contains the points of \( P \) that can reach and spend a positive amount of time in \( P' \), via a trajectory that remains within \( P \cup P' \) at all times, except for an intermediate time instant in which the trajectory may be in \( P \).

\[ \begin{align*}
\text{Cross}(P, \hat{P}, P') &= \{ x \in P \mid \exists f \in \text{Adm}^{\text{ua}}(x), 0 \leq \delta_1 < \delta_2 : \forall \delta \in (0, \delta_1) : f(\delta) \in P \land \\
&\quad \land \forall \delta \in (\delta_1, \delta_2) : f(\delta) \in P' \}. 
\end{align*} \]

Notice that the conditions above imply that \( f(\delta_1) \in cl(P) \cap cl(P') \).

Hence,

\[ \text{Cross}(P, \hat{P}, P') = \text{Cross}(P, \hat{P} \cap cl(P) \cap cl(P'), P'), \]

and we can assume w.l.o.g. that \( \hat{P} \subseteq cl(P) \cap cl(P') \).

We show in Section 6 that \( \text{Cross} \) is the main ingredient in a fixed point characterization of \( \text{RWA}^{\text{ua}} \). Sections 4 and 5 prove that \( \text{Cross}(P, P, P') \) is a polyhedron that can be computed using basic operations on convex polyhedra.

In the rest of the paper we always refer to the class of trajectories \( C_\circ \). Hence, we drop the corresponding superscript and write \( \text{Adm} \) for \( \text{Adm}^{\text{ua}} \) and \( \text{RWA} \) for \( \text{RWA}^{\text{ua}} \).

### 4. FROM GENERAL TRAJECTORIES TO STRAIGHT DIRECTIONS

As a first step towards the computation of the operator \( \text{Cross}(P, \hat{P}, P') \) defined in the previous section, we will show how to reformulate it in terms of straight trajectories only. The main results of this section and the next one are summarized in Figure 4.

We assume that we can compute the following basic operations on arbitrary convex polyhedra \( P, P' \): the Boolean operations \( P \cup P', P \cap P' \), and \( \overline{P} \); the topological closure \( cl(P) \) of \( P \); finally, the pre- and post-flows of \( P \), defined as follows. For a convex polyhedron \( P \), let:

\[ P \nearrow = \{ x - \delta c : x \in P, \delta \geq 0, c \in F \} \]
\[ P \nwarrow = \{ x - \delta c : x \in P, \delta \geq 0, c \in F \} \]
\[ P \searrow = \{ x + \delta c : x \in P, \delta \geq 0, c \in F \} \]
\[ P \swarrow = \{ x + \delta c : x \in P, \delta > 0, c \in F \} \]

Intuitively, the pre- and post-flow operators compute the pre- and post-image, respectively, of a convex polyhedron...
with respect to the straight directions contained in $F$. The algorithm for $P, \prec_0$ and $P, \ne_0$ can be found in [6].

It is well known that $P, \prec$ (resp., $P, \ne$) is not a convex polyhedron when $F$ is non-necessarily closed. The following example shows that the same is true even if both $P$ and $F$ are closed convex polyhedra. This observation contradicts a claim made by Halbachs et al. [9].

**Theorem 2.** Given two closed convex polyhedra $P$ and $F$, the following hold:
1. $P, \ne$ may not be a convex polyhedron;
2. $P, \prec = P \cup (P, \ne_0)$.

**Proof.** To show that the first property holds it suffices to consider the closed convex polyhedra $P = \{(0,0)\}$ and $F = \{(x,y) \mid x \geq 1\}$. According to the definition, $P, \ne = P \cup (P, \ne_0)$, which is a convex set but not a convex polyhedron. As to the second property, it is enough to observe that $P = \{x + \delta c \mid x \in P, \delta = 0, c \in F\}$.

We start by splitting $\text{Cross}(P, \hat{P}, P')$ into three simpler operators, according to the properties of the trajectory $f$ and the delay $\delta$ occurring in the definition of $\text{Cross}^0(P, P')$: $\text{Cross}^0(P, P')$ takes care of the case when $\delta = 0$; $\text{Cross}^+(P, P')$ takes care of the case when $\delta > 0$ and $f(\delta) \in P \cup P'$; finally, $\text{Cross}^+(P, \hat{P}, P')$ covers the remaining case, i.e., $\delta > 0$ and $f(\delta) \in \hat{P}$. Hence, it holds:

$$\text{Cross}(P, \hat{P}, P') = \text{Cross}^0(P, P') \cup \text{Cross}^+(P, P') \cup \text{Cross}^+(P, \hat{P}, P').$$

We recall the following result from the literature, which guarantees that every point reachable from a point $x$ along an admissible and differentiable trajectory can also be reached from $x$ along an admissible straight trajectory.

**Lemma 1.** [2] For all points $x \in \mathbb{R}^n$, if there is a trajectory $f \in \text{Adm}(x)$ and a time $\delta > 0$ such that $f(\delta) = y$, then there is a slope $c \in F$ such that $y = x + \delta c$.

The following result shows that $\text{Cross}^0$ can immediately be reformulated in terms of straight directions and easily computed with basic polyhedral operations. Given a set $P \subseteq \mathbb{R}^n$, we say that a trajectory $f$ lingers in $P$ if there exists $\delta > 0$ such that $f(\delta') \in P$ for all $0 < \delta' < \delta$.

**Theorem 3.** For all disjoint convex polyhedra $P, P'$, it holds:

$$\text{Cross}^0(P, P') = P \cap \text{cl}(P') \cap P' \prec.$$

**Proof.** First, notice that the definition of $\text{Cross}(P, \hat{P}, P')$ boils down to the following:

$$\text{Cross}^0(P, P') = \{x \in P \mid \exists f \in \text{Adm}(x), \delta > 0 : \forall \delta' \in (0, \delta] : f(\delta') \in P'\}.$$

Now, we can prove the two sides of the equivalence.

($\subseteq$) Let $x \in \text{Cross}^0(P, P')$ and let $f \in \text{Adm}(x)$ be the trajectory whose existence is postulated by the definition of $\text{Cross}^0$. Since $f$ lingers in $P'$, in each neighborhood of $x$ there is a point in $P'$. Hence, $x \in \text{cl}(P')$. Moreover, Lemma 1 implies that $x \in P' \prec$.

($\supseteq$) Let $x \in P \cap \text{cl}(P') \cap P' \prec$ and let $y \in P'$ such that $y = x + \delta c$, for suitable $\delta \geq 0$ and $c \in F$. Since $P$ and $P'$ are disjoint, it holds $\delta > 0$. Then, the trajectory $f(\delta) = x + \delta c$ lingers in $P'$ and proves that $x \in \text{Cross}^0(P, P')$.

Next, we show how $\text{Cross}^+(P, \hat{P}, P')$ can be expressed in terms of $\text{Cross}^+(P, \hat{P}, P')$ for a suitable $\hat{P}$. Let the boundary between $P$ and $P'$ be defined as:

$$\text{bdry}(P, P') = \text{cl}(P) \cap P' \cup (P \cap \text{cl}(P')).$$

It has been proved that $\text{bdry}(P, P')$ is a convex polyhedron [7].

**Lemma 2.** For all convex polyhedra $P, P'$, it holds:

$$\text{Cross}^+(P, P') = \text{Cross}^+(P, \text{bdry}(P, P'), P').$$

**Proof.** ($\subseteq$) Let $x \in \text{Cross}^+(P, P')$, according to the definition there exist a trajectory $f \in \text{Adm}(x)$ and two delays $\delta_1, \delta_2$ such that $f$ stays in $P'$ from 0 to $\delta_1$ (excluded), then $f(\delta_1) \in P \cup P'$, and finally $f$ lies in $P'$ from $\delta_1$ (excluded) to $\delta_2$. So, in each neighborhood of $f(\delta_1)$ there is both a point in $P$ and a point in $P'$. Hence, $f(\delta_1) \in \text{cl}(P) \cap \text{cl}(P')$ and therefore $f(\delta_1) \in \text{bdry}(P, P')$.

($\supseteq$) Conversely, let $x \in \text{Cross}^+(P, \text{bdry}(P, P'), P')$. The thesis follows immediately from the fact that $\text{bdry}(P, P') \subseteq P \cup P'$.

Lemma 2 implies that the only remaining task that we need to address is a way to compute $\text{Cross}^+(P, \hat{P}, P')$. As we shall show, this task turns out to be significantly involved. The first step towards the solution consists in reformulating $\text{Cross}^+$ in terms of straight trajectories. If we simply replace the arbitrary trajectory $f \in \text{Adm}(x)$ in the definition of $\text{Cross}^+$ with a straight trajectory of slope $c$, we obtain the following operator:

$$\text{StrCross}(P, \hat{P}, P') = \{x \in P \mid \exists c \in F, 0 < \delta_1 < \delta_2 : \forall \delta \in (0, \delta_1) : x + \delta c \in P \text{ and } x + \delta c \in \hat{P} \text{ and } \forall \delta \in (\delta_1, \delta_2) : x + \delta c \in P'\}.$$ Intuitively, these are the points of $P$ which can reach a point in $P'$ following a straight direction while remaining in $P \cup P'$ at all times, except in a single point of $\hat{P}$.

Clearly, $\text{StrCross}(P, \hat{P}, P') \subseteq \text{Cross}^+(P, \hat{P}, P')$. In addition, any point in $P$ which can reach $\text{StrCross}(P, \hat{P}, P')$ also belongs to $\text{Cross}^+(P, P', P')$:

**Lemma 3.** For all convex polyhedra $P, \hat{P}$ and $P'$ the following holds:

$$P \cap \text{StrCross}(P, \hat{P}, P') \subseteq \text{Cross}^+(P, \hat{P}, P').$$

To prove Lemma 3, we shall need the following result, which shows how to connect, in an admissible and differentiable fashion, two points which can be connected by the concatenation of two straight-line trajectories. Due to space constraints, the proof of the following lemma, as well as those of several other results, can be found in the Appendix.

**Lemma 4 (INTERPOLATION).** Given three points $x_0, x_1, x_2 \in \mathbb{R}^n$, two directions $c_0, c_1 \in F$ and two delays $\delta_0, \delta_1 \geq 0$ such that $x_1 = x_0 + \delta_0 c_0$ and $x_2 = x_0 + \delta_1 c_1$, there exists a trajectory $f \in \text{Adm}(x_0)$ such that $f(0) = x_0$, $f(\delta_0 + \delta_1) = x_2$, $f'(\delta_0) = c_1$, and $f(\delta)$ is a strict convex combination of $x_0, x_1, x_2$ for all $\delta \in (0, \delta_0 + \delta_1)$.
Figure 2: When a point $x \in P$ can reach another point $y$ which is in $\text{StrCross}(P, P, P')$, $x$ can differentiably cross into $P'$ (see Lemma 3). Here, $\hat{P} = \{z\}$.

**Proof of Lemma 3.** Let $x \in P \cap \text{StrCross}(P, \hat{P}, P') \not\owns y$. The proof is illustrated in Figure 2. Let $y \in \text{StrCross}(P, \hat{P}, P')$ such that $x \in \{y\} \not\owns \hat{P}$. There exist $c \in F$ and $0 < \delta_1 < \delta_2$ satisfying the definition of $\text{StrCross}(P, \hat{P}, P')$ for $y$. Let $z = y + \delta_1 c$, by construction it holds $z \in \hat{P} \cap \overline{cl}(P) \cap cl(P')$. By applying Lemma 4 with $x_0 = x$, $x_1 = y$, and $x_2 = z$, we get a differentiable trajectory $f$ in $\text{Adm}(x)$ from $x$ to $z$ whose derivative in $z$ is $c$. Moreover, $f$ is contained in $P$, with the possible exception of $z \in \hat{P}$. Therefore, the concatenation of $f$ and the straight trajectory $g(\delta) = z + \delta c$ is everywhere differentiable and crosses into $P'$. As a consequence, $x \in \text{Cross}^+(P, P, P')$.

While Lemma 3 provides a sound approximation of $\text{Cross}^+$ in terms of straight trajectories, it does not, unfortunately, ensure completeness. Indeed, there may be points that belong to $\text{Cross}^+(P, P, P')$ but not to $\text{StrCross}(P, P, P') \owns \hat{P}$.

Figure 3: Reaching points in $\text{StrCross}$ is not necessary to be in $\text{Cross}^+$.

Consider the situation depicted in Figure 3, where $P$ and $P'$ are open convex polyhedra, $\hat{P}$ contains a single point $z$ (the upper right corner of the closure of $P$), and the line segment $A$ (which does not include $\hat{P}$) is a region to avoid. Given the flow constraint depicted on the right-hand side of the figure, it holds $\text{StrCross}(P, \hat{P}, P') = \emptyset$, as no straight trajectory leads from $P$ to $P'$ passing through $\hat{P}$.

Notice, however, that the point $z_1$, lying in the closure of $P'$, is reachable from $x$ by following a straight trajectory which always remains in the closure of $P'$. Then, a straight trajectory, with derivative $c$, leads from $z_1$ to a point $z_2$, which lies in the closure of $P'$, without ever leaving the closures of the two polyhedra. Finally, $z_2$ can reach $y$ in $P'$, following a straight trajectory that never leaves the closure of $P'$. Therefore, Lemma 4, applied with $x_0 = x$, $x_1 = z_1$, and $x_2 = z_2$, gives a differentiable trajectory from $x$ to $z_2$, which never leaves $P$ except for the end point $z_1 \in \hat{P}$ and whose derivative in $z_2$ is $c$ (the straight direction from $z_1$ to $z_2$). Similarly, another application of Lemma 4, this time applied to $x_0 = z$, $x_1 = z_2$, and $x_2 = y$, gives a differentiable trajectory from $z$ to $y$, which never leaves $P'$ except for the starting point $z \in \hat{P}$ and whose derivative in $z$ is, again, $c$. The concatenation of these two trajectories in $z$ is depicted in Figure 3 and is a differentiable trajectory from $x$ to $y$ which never leaves $P \cup P'$ except for the single point $z \in \hat{P}$. Hence, we have that $x \in \text{Cross}^+(P, \hat{P}, P')$.

This example suggests that the straight trajectory reformulation of Lemma 3, while not complete, can be extended, exploiting Lemma 4, by also allowing certain straight trajectories lying in the closures of $P$ and $P'$. We, therefore, obtain the following operator:

$$\text{ClosCross}(P, \hat{P}, P') = \{x \in cl(P) \cap P' \mid \exists c \in F, 0 < \delta_1 < \delta_2 :$$

$$\forall \delta \in (0, \delta_1) : x + \delta c \in cl(P)$$

$$x + \delta_1 c \in \hat{P}$$

$$\forall \delta \in (\delta_1, \delta_2) : x + \delta c \in cl(P')$$

$$x + \delta_2 c \in cl(P') \cap P' \not\owns \hat{P} \}. \not\owns \hat{P}$$

The following theorem ensures that $\text{ClosCross}$ allows us to obtain a sound and complete reformulation of $\text{Cross}^+$ in terms of straight trajectories.

**Theorem 4.** For all convex polyhedra $P, \hat{P}$ and $P'$ the following holds:

$$\text{Cross}^+(P, \hat{P}, P') = P \cap \text{ClosCross}(P, \hat{P}, P') \not\owns \hat{P}$$

Before proving Theorem 4, we need an additional result, connecting arbitrary trajectories and straight trajectories. Consider a differentiable trajectory lying within a convex polyhedron $P$. Along any tangent to the curve one can find a point that is still in the closure of $P$ (if not in $P$ itself) and that is reachable from the initial point of the curve. The following lemma formalizes this property.

**Lemma 5 (Tangent).** Let $P$ be a convex polyhedron, $x$ a point, $f \in \text{Adm}(x)$ a trajectory, and $\delta > 0$ a delay such that in all non-empty intervals $(\delta, \delta')$ there is a time $\gamma$ such that $f(\gamma) \in P$. Then, there exists $\delta' > 0$ such that $f(\delta) + \delta c \in cl(P) \cap cl(P')$.

**Proof of Theorem 4.** (1) This part of the proof has been illustrated in the above discussion regarding the example in Figure 3. A full proof is provided in the Appendix. (2) Let $x \in \text{Cross}^+(P, \hat{P}, P')$ and let $f \in \text{Adm}(x)$ and $\delta_1, \delta_2$ be the trajectory and the delays whose existence is postulated by the definition of $\text{Cross}^+$. By definition, $x \in P$. Let $y = f(\delta_1)$, recall that $y \in \hat{P}$. Moreover, since $f(\delta) \in P$ for all $\delta \in [0, \delta_1)$, we also have that $y \in cl(P)$.

Let $c = f(\delta_1) \in F$, by Lemma 5, there exists $\gamma_1 > 0$ such that $u_1 \triangleq y - \gamma_1 c \in cl(P) \cap \{x\}$. Since $u_1 \in cl(P)$ and $y \in cl(P)$, then for all $y \in [0, \gamma_1)$ we have $u_1 + \delta c \in cl(P)$.

Similarly, by applying Lemma 5 backwards from a point $f(\delta) \in P'$ (it is sufficient to consider any $\delta \in (\delta_1, \delta_2)$), we obtain another value $\gamma_2 > 0$, such that $u_2 \triangleq y + \gamma_2 c \in cl(P') \cap cl(P')$. Since $y \in cl(P')$ and $u_2 \in cl(P')$, then for all $\delta \in (\gamma_1, \gamma_1 + \gamma_2)$ we have $y + \delta c \in cl(P')$. As a consequence, we obtain that $x \in P \cap \text{StrCross}(P, \hat{P}, P') \not\owns \hat{P}$.

In conclusion, Theorems 3 and 4 allow us to compute $\text{Cross}(P, \hat{P}, P')$ provided we can compute $\text{ClosCross}(P, \hat{P}, P')$, or at least its pre-flow. Indeed, that is the subject of the following section.
5. COMPUTING THE Cross+ OPERATOR

We start by introducing some preliminary geometric notions.

5.1 Geometric Primitives

An affine combination of two points \( x \) and \( y \) is any point \( z = ax + (1-a)y, \) for \( a \in \mathbb{R} \). An affine set is any set of points closed under affine combinations. The empty set, a single point, a line, a hyper-plane, and the whole ambient space are all examples of affine sets. Given a convex polyhedron \( P \), the affine hull of \( P \), denoted \( ahull(P) \), is the smallest affine set containing \( P \).

Given a polyhedron \( P \subseteq \mathbb{R}^n \), the affine dimension of \( P \) is the natural number \( k \leq n \), such that the maximum number of affinely independent points in \( P \) is \( k+1 \).

The relative interior of a convex polyhedron \( P \), denoted \( rint(P) \), is the interior of \( P \) taken in the space corresponding to the affine hull of \( P \) itself. More formally, \( x \in rint(P) \) if and only if there is a ball \( N_\epsilon(x) \) of radius \( \epsilon > 0 \) centered in \( x \), such that \( N_\epsilon(x) \cap ahull(P) \subseteq P \).

Similarly, given a polyhedron \( P \), we call the set \( N \) a relative neighborhood of a point \( x \in P \), if there is a ball \( N_\epsilon(x) \) of radius \( \epsilon > 0 \), such that \( N_\epsilon(x) \cap ahull(P) \subseteq P \). Intuitively, the relative neighborhood of \( x \) is a neighborhood of \( x \) relative to the affine hull of \( P \).

The point reflection of a point \( x \) w.r.t. a point \( y \), in symbols \( mirror(x,y) \), is the point \( y \) itself, beyond \( y \) along the line connecting \( x \) and \( y \), such that \( \|y-x\| = \|x-y\| \). Similarly, one can define the reflection \( mirror(x,Q) \) of \( x \) w.r.t. an affine set \( Q \). More precisely, \( mirror(x,Q) \) is defined as the point reflection of \( x \) w.r.t. the orthogonal projection of \( x \) on \( Q \). Finally, the above definitions can be extended to sets of points \( P \), giving rise to the reflections \( mirror(P,y) \) and \( mirror(P,Q) \). For a convex polyhedron \( Q \) which is not necessarily an affine set, we will abuse the notation and write \( mirror(P,Q) \) when we mean \( mirror(P, ahull(Q)) \).

The affine hull and the relative interior can be easily computed using the standard “double description” of convex polyhedra via constraints and generators [3]. Moreover, it is well known that the reflection of a point w.r.t. a given affine set is a linear transformation, and as such it is exactly computable starting from a representation of the affine set. The details are beyond the scope of the present paper.

5.2 Computation of Cross+

In Section 4 we have reduced the problem of computing the set \( \text{Cross}^+(P,\hat{P},P') \) to the problem of computing (the pre-flow of) \( \text{ClosCross}(P,\hat{P},P') \), with \( \hat{P} \) a convex polyhedron and \( \hat{P} \subseteq cl(P) \cap cl(P') \). In the rest of the section, we shall then assume that \( \hat{P} \) is any convex polyhedron contained in the closures of \( P \) and \( P' \).

The main difficulty we have to face in order to compute \( \text{ClosCross}(P,\hat{P},P') \) is to ensure that the points collected in the set can actually cross from \( P \) to \( P' \) following a “single” admissible straight direction in \( F \). Clearly, if a point \( y \in cl(P) \) can reach a point \( x \in \hat{P} \) along a straight direction \( c \in F \), i.e., \( x = y + \delta c \) for some \( \delta > 0 \), then its point reflection w.r.t. \( x \), namely \( mirror(y,x) \), is reachable from \( y \) along the same admissible direction, indeed \( mirror(y,x) = y + 2\delta c \). For instance, in Figure 5 if point \( y \) can reach point \( x \) along a straight direction, then it can also reach its point reflection \( y' \) (w.r.t. \( x \)) along the same direction.

The observation above motivates the definition:

\[
\text{MirCross}(P,x,P') = cl(P) \cap P \cap \{x\} \cup \text{mirror}(cl(P') \cap P',x).
\]

The set \( \text{MirCross}(P,x,P') \) collects all the points of the closure of \( P \), reachable from \( P \), that can reach, following a single straight trajectory passing through \( x \), some point of the portion of the closure of \( P' \) that can, in turn, reach \( P' \).

In addition, when \( x \in cl(P) \cap cl(P') \), any point belonging to \( \text{MirCross}(P,x,P') \) can reach, following a single straight trajectory, some point in \( cl(P') \cap P' \), never leaving \( cl(P) \cup cl(P') \), as required by the definition of \( \text{ClosCross}(P,\hat{P},P') \). As a consequence, a point belongs to \( \text{MirCross}(P,x,P') \) if and only if it belongs to \( \text{ClosCross}(P,\hat{P},P') \). This approach ensures that, when \( \hat{P} \) contains a single point, we can compute the set of points in \( \text{ClosCross}(P,\hat{P},P') \) that cross from \( P \) to \( P' \) along a straight direction passing through \( P \).

By generalizing the operator \( \text{MirCross} \) to take an arbitrary convex polyhedron \( Q \) as second argument, we obtain the following:

\[
\text{MirCross}(P,Q,P') = cl(P) \cap P \cap \{Q\} \cup \text{mirror}(cl(P') \cap P',Q).
\]

The set \( \text{MirCross}(P,Q,P') \) is a convex polyhedron containing the closures of the portion of \( P \) which: (i) \( x \) are reachable (along a straight trajectory) from \( P \), (ii) \( x \) can reach a point in \( Q \) in a positive amount of time along a straight direction, and (iii) \( x \) have a reflection w.r.t. the affine hull of \( Q \) which lies in the portion of the closure of \( P' \) that can reach \( P' \).

It is important to notice that, differently from the case of a single point, the straight trajectory reaching \( Q \) from a point \( x \in cl(P) \cap P \), which is clearly admissible, need not be the same straight line connecting \( x \) and \( Q \) with its reflection w.r.t. \( Q \). Even worst, this straight line may not even be an admissible trajectory. Figure 5 shows that the point reflection \( y' \) of \( y \) w.r.t. \( x \) may be different from the reflection of \( y \) with respect to \( Q \) even when \( x \in Q \).

The following result, however, ensures that, if \( Q \) is an open set w.r.t. its affine hull, namely when \( Q = rint(Q) \), and \( Q \subseteq cl(P') \cap cl(P') \), then for all \( x \in Q \), any point in the set \( \text{MirCross}(P,Q,P') \) can reach some point in the set \( \text{MirCross}(P,Q,P') \), and vice versa.

\[1\text{It is easy to verify that } cl(P) \cap P \text{ is a convex polyhedron even when } P \text{ is not.}\]
LEMMA 6. For all convex polyhedra $P, P', Q \subseteq cl(P) \cap cl(P')$ such that $Q = rint(Q)$, points $x \in Q$, and directions $c \in F$, let $D_Q$ (resp., $D_x$) be the set of delays $\delta > 0$ such that $x - \delta c \in \text{MirCross}(P, Q, P')$ (resp., $x - \delta c \in \text{MirCross}(P, x, P')$). Then, either $D_Q = D_x = \emptyset$ or both $D_Q$ and $D_x$ are non-empty intervals having the infimum $0$.

As a consequence of Lemma 6, whenever $\hat{P}$ is the relative interior of itself and is included in $cl(P) \cap cl(P')$, a point in the closure of $P$ can reach the closure of $P'$ following a single straight trajectory passing through $\hat{P}$ if and only if it can reach a point in $\text{MirCross}(P, \hat{P}, P')$. It is now easy to solve the problem for a general convex polyhedron $\hat{P}$ which is not a relative interior. It suffices to recursively decompose $\hat{P}$ into convex polyhedra $Q$, each of which is the relative interior of itself, and compute $\text{MirCross}(P, Q, P')$ for each such component. This leads to the following operator, called $\text{RMirCross}$ for recursive:

$$\text{RMirCross}(P, \hat{P}, P') = \text{MirCross}(P, \text{rint}(\hat{P}), P') \cup \bigcup_{Q \subseteq \{P \cap \text{rint}(\hat{P})\}} \text{RMirCross}(P, Q, P').$$

The operator can easily be computed by a recursive algorithm, whose termination is guaranteed by noticing that for every $Q \in \{\hat{P} \cap \text{rint}(\hat{P})\}$, the affine dimension of $Q$ is strictly lower than the affine dimension of $\hat{P}$, down to the case where $Q$ contains a single point, in which case $Q$ is the relative interior of itself and the recursion terminates.

As an example, Figure 6 depicts sets $\text{RMirCross}(P, \hat{P}, P')$, $\text{ClosCross}(P, \hat{P}, P')$ and $\text{Cross}^+(P, \hat{P}, P')$, assuming that the upper extreme of the segment labeled $\hat{P}$ actually belongs to $\hat{P}$, while the lower one does not. Dashed boundaries identify topologically open sides of polyhedra. It is easy to verify that no admissible differentiable trajectory can cross from a point along the dashed boundaries of $C_1 \cup C_2$ to $P'$ passing through $P$, hence they belong neither to $\text{ClosCross}(P, P, P')$ nor to $\text{Cross}^+(P, \hat{P}, P')$. The reason why they do not belong to $\text{RMirCross}(P, \hat{P}, P')$ is that the operator considers the relative interior of $\hat{P}$ first, collecting $C_1$. Then, it recursively considers the upper extreme point of $\hat{P}$, say $x$. The resulting set $\text{RMirCross}(P, x, P')$ is empty, as none of the points of $P$ that can reach $x$ (namely, the points along the upper boundaries of $C_1$ and $C_2$ and below) has a point reflection w.r.t. $x$ lying in the closure of $P'$.

![Figure 6: Difference between ClosCross and RMirCross. We have $C_1 = \text{RMirCross}(P, \hat{P}, P')$, $C_1 \cup C_2 = \text{ClosCross}(P, \hat{P}, P')$, and $C_1 \cup C_2 \cup C_3 = \text{Cross}^+(P, \hat{P}, P')$.](image)

The following lemma ensures that a point can reach the set $\text{ClosCross}(P, \hat{P}, P')$ if and only if it can reach the set $\text{RMirCross}(P, \hat{P}, P')$, allowing us to obtain the desired result:

**LEMMA 7.** Let $P$, $\hat{P}$ and $P'$ be convex polyhedra, with $P \subseteq cl(P) \cap cl(P')$, then

$$\text{ClosCross}(P, \hat{P}, P') \subseteq \text{RMirCross}(P, \hat{P}, P').$$

**Proof.** (\(\subseteq\)) Let $x \in \text{RMirCross}(P, \hat{P}, P')$. Then, there is a point $y \in \text{RMirCross}(P, \hat{P}, P')$, which is reachable from $x$. Hence, there must be a polyhedron $Q \subseteq \hat{P}$, with $Q = \text{rint}(Q)$ and $y \in \text{MirCross}(P, Q, P')$. By the definition of $\text{MirCross}(P, Q, P')$, $y$ must belong to $cl(P)$, must be reachable from $P$, and must reach a point in $z \in Q$ along a straight direction $c \in F$ in a positive amount of time $\delta > 0$ (i.e., $z = y + \delta c$). Clearly, the set of delays $D_Q$ of Lemma 6 contains at least $\delta$, since $z - \delta c = y \in \text{MirCross}(P, Q, P')$. Therefore, Lemma 6 ensures that both $D_Q$ and $D_x$ are non-empty time intervals with infimum $0$. Let $\delta_1$ be any time instant contained in $D_x$ and $\delta' = \min(\delta, \delta_1) > 0$. Then, let $y' = z - \delta' c \in cl(P)$, it holds $y' \in \text{MirCross}(P, z, P')$. As a consequence, $y' \in cl(P) \cap P'$, it can reach $z$ in a positive amount of time $\delta'$ along direction $c$, and in time $2\delta'$, along the same direction $c$, it can reach a point in $cl(P) \cap P'$. This gives us a point $y' \in \text{ClosCross}(P, \hat{P}, P')$. Finally, we obtain the thesis $x \in \text{ClosCross}(P, \hat{P}, P')$, by observing that, since $x$ reaches $y'$ along a direction in $F$ and $y'$, in turn, reaches $y'$ along some direction in $F$, also $x$ reaches $y'$ along a direction in $F$.

(\(\supseteq\)) As to the other direction, let $x \in \text{ClosCross}(P, \hat{P}, P')$. This means that $x$ reaches a point $y \in cl(P) \cap P'$. In addition, there are two positive delays $0 < \delta_1 < \delta_2$ and a direction $c \in F$, such that $y + \delta c \in cl(P)$ for all $\delta \in (0, \delta_1)$, $y + \delta c \in cl(P')$ for all $\delta \in (\delta_1, \delta_2)$, $z \triangleq y + \delta_1 c \in \hat{P}$ and $y' \triangleq y + \delta_2 c \in cl(P) \cap P'$. Let $\delta' = \min(\delta_1, \delta_2 - \delta_1)$. Clearly, the point $z_1 = z + \delta' c \in cl(P')$ is reachable from $y$ along direction $c$, hence from $x$ as well. Similarly, the point $z_2 \triangleq z + \delta' c \in cl(P')$ can reach $y'$ along direction $c$, hence also any point reachable from $y'$ in $P'$. It is immediate to verify that $z_1 = \text{mirror}(z_2, z) \subseteq \text{mirror}(cl(P') \cap P', z)$. We, then, obtain that $z_1 \in \text{MirCross}(P, z, P')$. Since, however, $z \in \hat{P}$,
there is a \( Q \subseteq \hat{P} \), with \( Q = \text{rint}(Q) \) and which contains \( z \).
Now, the application of Lemma 6 gives us a point \( z'_1 \) (possibly different from \( z_1 \)), such that \( z'_1 \in \text{MirCross}(P, Q, P') \subseteq \text{RMirCross}(P, \hat{P}, P') \) which is reachable from \( z_1 \) along direction \( c \). Therefore, \( z_1 \) is reachable also from \( y \), along the same direction. Once again, since \( x \) reaches \( y \), which, in turn, reaches \( z'_1 \), also \( x \) can reach \( z'_1 \) and we obtain that \( x \in \text{RMirCross}(P, \hat{P}, P') \), as desired.

In conclusion, for all convex polyhedra \( P, \hat{P} \) and \( P' \), whenever \( \hat{P} \subseteq \text{cl}(P) \cap \text{cl}(P') \) we can compute \( \text{Cross}^+(P, \hat{P}, P') \) by means of the following:

\[
\text{Cross}^+(P, \hat{P}, P') = P \cap \text{RMirCross}(P, \hat{P}, P')'.
\]

### 6. FIXPOINT CHARACTERIZATION OF REACH-WHILE-AVOIDING

In this section, we show how to use the Reach and Cross operators to compute \( \text{RWA}^{\text{Gd}} \). Analogously to the \( \tau_{ae} \) operator, we define the following:

\[
\tau_0(G, A, W) = G \cup \bigcup_{P \in [\mathbb{P}]} \text{Reach}(P, G) \cup \bigcup_{P \in [\mathbb{P}]} \text{Cross}(P, \hat{P}, P').
\]

We prove that a finite number of repeated applications of \( \tau_0(G, A, W) \), starting from \( W = \emptyset \), capture exactly all points in \( \text{RWA}^{\text{Gd}}(G, A) \).

**Theorem 5.** For all convex polyhedra \( G \) and polyhedra \( A \), such that \( G \cap A = \emptyset \), we have

\[
\text{RWA}^{\text{Gd}}(G, A) = \mu W \cdot \tau_0(G, A, W).
\]

Moreover, the fixpoint is reached in a finite number of iterations.

As before, let

\[
W_0 = \emptyset \quad W_{i+1} = \tau_0(G, A, W_i).
\]

In order to prove the above theorem, we proceed as follows. First, in Section 6.1 we prove that there is a normal form for witnesses, which in turn induces a partition of \( \text{RWA}(G, B) \) into a finite number of classes \( R_0, \ldots, R_k \). Then, in Section 6.2, we show that the points belonging to the class \( R_i \) are included in the \((i + 1)\)-th iteration of the fixpoint (1), i.e., to \( W_{i+1} \). Finally, in Section 6.3 we prove that whenever \( W \) is a subset of \( \text{RWA}(G, A) \), \( \tau_0(G, A, W) \) is also a subset of \( \text{RWA}(G, A) \). Together, these results imply that \( W_{k+1} \) coincides with \( \text{RWA}(G, B) \).

#### 6.1 Canonicity

In this section, we introduce a normal form for witnesses. For a point \( x \in \text{RWA}(G, A) \) and a witness \( \xi = (f, \delta_f) \) for \( x \), for all \( \delta \) between \( 0 \) and \( \delta_f \), \( f(\delta) \) lies in one of the convex polyhedra that constitute \( \overline{A} \). In general, a witness can enter in and exit from the same polyhedron \( P \in [\overline{A}] \) an unbounded number of times. However, we prove that there are special witnesses, called \( \overline{A} \)-canonical, that do not spend a positive amount of time more than once in the same polyhedron.

Given a witness \( \xi = (f, \delta_f) \) and a convex polyhedron \( P \), let \( \Delta^f_\delta \) be the set of delays \( \delta \leq \delta_f \) such that \( f \) lies in \( P \) in an open interval around \( \delta \). Formally,

\[
\Delta^f_\delta = \{ 0 \leq \delta \leq \delta_f \mid \exists \gamma > 0 \forall \delta' \in (\delta - \gamma, \delta + \gamma) : f(\delta') \in P \}.
\]

We say that a witness \( \xi = (f, \delta_f) \) for \( x \) is \( P \)-canonical if either \( \Delta^f_\delta = \emptyset \) or \( f(\delta) \in P \) for all \( \delta \in (\inf \Delta^f_\delta, \sup \Delta^f_\delta) \). The definition implies that once a \( P \)-canonical witness spends a positive amount of time in \( P \) and then exits from it, it can only return to \( P \) for instantaneous visits (i.e., in isolated time points).

For a non-convex polyhedron \( B \), we say that the witness \( \xi \) is \( B \)-canonical if it is \( P \)-canonical for all \( P \in [B] \).

**Lemma 8.** (Canonicity). For all \( x \in \text{RWA}(G, A) \) there exists an \( \overline{A} \)-canonical witness for \( x \).

If a witness \( \xi = (f, \delta_f) \) lies entirely within a polyhedron \( B \) (i.e., \( f(\delta) \in B \) for all \( \delta \in [0, \delta_f] \)), it induces a partition of the interval \([0, \delta_f]\) in a possibly infinite sequence of intervals \( I_0, I_1, \ldots, I_\alpha, \ldots \) such that \( f \) lies in the same patch \( P_\alpha \in [B] \) during each interval \( I_\alpha \) and two subsequent polyhedra are distinct (i.e., we do not partition more often than necessary).

We call the sequence of pairs \( (I_\alpha, P_\alpha) \) the B-segmentation of \( \xi \). Notice that for all pairs of subsequent intervals \( I_\alpha, I_{\alpha+1} \), at most one of them is singular (i.e., of length 0).

Consider the B-segmentation of a \( B \)-canonical witness. For all patches \( P \in [B] \), there is at most one non-singular time interval during which the witness lies in \( P \). Since every other interval in the sequence must be non-singular, the segmentation can contain at most \( 2|B| + 1 \) intervals (i.e., \([B]|-\text{non-singular intervals interleaved with } [B]|+1 \text{ singular ones} \)). Now, for a witness \( \xi \) define \( \text{rank}(\xi) \) as the length (i.e., the order type) of its \( \overline{A} \)-segmentation, and \( \text{rank}(x) \) the minimum rank of all witnesses for \( x \). In light of Lemma 8 and the above discussion, we obtain the following result.

**Corollary 1.** For all points \( x \in \text{RWA}(G, A) \), it holds \( \text{rank}(x) \leq 2|\overline{A}| + 1 \).

The above corollary provides the main reason why our fixpoint procedure terminates. However, in order to prove that our fixpoint characterization is complete, we need more than \( \overline{A} \)-canonicity. We also need witnesses to be canonical w.r.t. the intermediate results of the computation, i.e., the sets \( W_i \) of Equation 2. Hence, we introduce the following definition and the corresponding lemma.

We say that a polyhedron \( B \) refines \( \overline{A} \) if for all \( P \in [B] \) there exists \( P' \in [\overline{A}] \) such that \( P \subseteq P' \). Notice that this implies \( B \subseteq \overline{A} \).

**Lemma 9.** Let \( B \) be a refinement of \( \overline{A} \). Then, for all \( x \in \text{RWA}(G, A) \) there exists a \( B \)-canonical witness \( \xi \) such that \( \text{rank}(\xi) = \text{rank}(x) \).

\( B \)-canonicity is a sort of regularity condition w.r.t. the internal boundaries of \( B \) (i.e., the boundaries between different patches of \( B \)). The following lemma formalizes this regularity.

**Lemma 10.** For all polyhedra \( B \), if a witness \( \xi = (f, \delta_f) \) is contained in \( B \) and it is \( B \)-canonical then for all \( \delta \in [0, \delta_f] \) there exists a non-empty open time interval \((\delta, \delta + \gamma)\) during which \( f \) lies in the same polyhedron \( P \in [B] \).

\(^2\)In fact, the order type of this sequence may be greater than \( \omega \), so that the sequence needs to be indexed by ordinals.
6.2 Completeness

We can now prove that all points in $\text{RWA}(G, A)$ will be eventually included in the fixed point (1).

**Theorem 6 (Completeness).** Let $x \in \text{RWA}(G, A)$, $r = \text{rank}(x)$, and let $W_i$ be defined as in (2), for all $i \geq 0$. If $r = 0$ then $x \in W_1$ and if $r > 0$ then $x \in W_r$.

**Proof.** First, we assume w.l.o.g. that $G$ is one of the patches of $A$. If this is not the case, modify $[A]$ as follows: replace each $P \in [A]$ with $[P \setminus G]$; then, add $G$ as an extra patch.

Let $x \in \text{RWA}(G, A)$. If $\text{rank}(x) = 0$ then there exists a witness for $x$ that is entirely contained in $G \in [A]$. Then, by definition of $\tau_A$ we have $x \in \tau_A(G, A, \emptyset) = W_1$.

For the higher values of $r$ we proceed by induction. If $\text{rank}(x) = 1$, there exists a witness $\xi = (f, \delta_f)$ for $x$ that is entirely contained in two patches $P, G \in [A]$. More precisely, $f(\delta_f) \in G$ and $f(\delta) \in P \cup G$ for all $\delta \in [0, \delta_f]$. Hence, it holds $x \in \text{Reach}(P, G) \subseteq \tau_A(G, A, \emptyset) = W_1$.

Next, assume that $\text{rank}(x) = r + 1 > 1$. We apply Lemma 9 to $x$ and $W_r$. This is legitimate, as $W_r$ can be represented in a way that refines $A$. Indeed, according to the definition of $\tau_A$, $W_r$ is the union of several other polyhedra, each of which is included in some $P \in [A]$.

Then, by Lemma 9 there exists a witness $\xi = (f, \delta_f)$ for $x$ that is $W_r$-canonical and such that $\text{rank}(\xi) = r + 1$. Let $(\bar{I}_i, P_i)_{i=0, r+1}$ be the $A$-segmentation of $\xi$. We distinguish the following cases.

1. $I_0 = [0, 0] = \{0\}$, i.e., $f$ immediately leaves the first polyhedron $P_0$. In this case, for all $\delta \in I_1$ the rank of $f(\delta)$ is at most $r$ because the suffix of $f$ starting from $\delta$ is a witness for $f(\delta)$ and its rank is $r$. By inductive hypothesis, it holds $f(\delta) \in W_r$. Since $\xi$ is $W_r$-canonical, by Lemma 10 $f$ lingers in some $P' \in [W_r]$. Hence, $f$ proves that $x \in \text{Cross}^0(P_0, P') \subseteq \tau_A(G, A, W_r) = W_{r+1}$.

2. $I_0 \neq \{0\}$, i.e., $f$ lingers in $P_0$. Let $\delta_0$ be the right extreme of $I_0$, for all $\delta \in (\delta_0, \delta_f)$ it holds $\text{rank}(f(\delta)) \leq r$. By inductive hypothesis, $f(\delta) \in W_r$. By Lemma 10, applied to $\xi$ and $\delta$, there exists a non-empty time interval $(\delta_0, \delta_0 + \gamma)$ and a patch $P' \in [W_r]$ such that $f(\delta) \in P'$ for all $\delta \in (\delta_0, \delta_0 + \gamma)$. If $I_0$ is right-closed, i.e., $I_0 = [0, \delta_0]$, then $f(\delta_0) \in P_0$. Then, $f$ proves that $x \in \text{Cross}^+(P_0, P_0, P') \subseteq W_{r+1}$.

Otherwise, $\text{rank}(f(\delta_0)) \leq r - 1$ and, therefore, by inductive hypothesis $f(\delta_0) \in W_r$. In particular, let $\hat{P} \in [W_r]$ be the patch such that $f(\delta_0) \in \hat{P}$. Then, $f$ proves that $x \in \text{Cross}^+(P_0, \hat{P}, P') \subseteq W_{r+1}$.

6.3 Correctness

The following auxiliary result states that from each point in $\text{RWA}(G, A)$ there is a witness trajectory that follows a straight line for a positive amount of time.

**Lemma 11.** For all $x \in \text{RWA}(G, A)$ there exist a witness $(f, \delta_f)$, a delay $\delta^* \leq \delta_f$, and a slope $c \in F$ such that $f(\delta) = c$ for all $\delta \in [0, \delta^*)$.

With the result given by the lemma above, we are now ready to prove that the fix-point procedure is correct, namely that at any iteration of the procedure the operator $\tau_A$ only adds points which belong to $\text{RWA}(G, A)$.

**Theorem 7 (Incremental correctness).** For all convex polyhedra $G$ and polyhedra $A$ and $W$, such that $G \cap A = \emptyset$ and $W \subseteq \text{RWA}(G, A)$, it holds $\tau_A(G, A, W) \subseteq \text{RWA}(G, A)$.

**Proof.** Let $x \in \tau_A(G, A, W)$. If $x \in \bigcup_{P \in \text{Reach}(P, G)} \text{Cross}(P, \hat{P}, P')$, it is easy to verify that either $x \in G$ or there is a straight-line trajectory that starts from $x$ and reaches $G$ without hitting $A$. Otherwise, it holds $x \in \bigcup_{P \in \text{Reach}(P, G)} \bigcup_{P, P' \in [W]} \text{Cross}(P, \hat{P}, P')$.

In particular, let $P \in [A]$ and $P, P' \in [W]$ be such that $x \in \text{Cross}(P, P, P')$. We distinguish two cases based on the definition of $\text{Cross}$.

1. $x \in \text{Cross}^0(P, P')$. This case is illustrated by Figure 7. According to the definition of $\text{Cross}^0$, let $f \in \text{Adm}(x)$ and $d > 0$ be such that $f(\delta) \in P'$ for all $\delta \in (0, \delta)$. Notice that $f$ shows that $x \in c(P')$, because in every neighborhood of $x$ there is a point in $P'$.

By Lemma 1, there is a slope $c \in F$ and a delay $\gamma > 0$ such that $f(\gamma) = x + \gamma c$. Consider an arbitrary point $x'$ of the type $x + \delta c$, for $0 < \delta \leq \gamma$. Being a convex combination of a point in $c(P')$ and a point in $P'$ different from $x$, $x'$ belongs to $P'$. By Lemma 11, $x'$ has a witness that starts with a straight line segment, and this witness must linger in one of the patches in $[A]$. Hence, there exists a delay $\delta < \gamma$ and a patch $P'' \in [A]$ such that all points $x + \delta c$, for $0 < \delta < \delta'$, have a witness that starts with a straight line segment and lingers in $P''$ (it may be $P'' = P'$). Let $\xi = (g, \delta_g)$ be such a witness for the point $y = x + \delta c$. By construction, there exists $\delta^* > 0$ such that $g(\delta') \in P''$ for all $0 < \delta < \delta'$ and moreover $g$ follows a straight line segment of a given slope $c' \in F$ at all times between $0$ and $\delta^*$. Let $z = g(\delta^*)$. By applying Lemma 4 to points $x_0 = x$, $x_1 = y$, and $x_2 = z$, we obtain a trajectory $f'$ that starts in $x$ and reaches $z$ with final slope $c'$. Moreover, each point of $f'$ (except its extremes) is a strict convex combination of two points in $c(P'')$ (namely, $x$ and $y$) and a point in $P''$ (namely, $z$); hence it belongs to $P''$. Finally, $f'$ can be connected to $g$ at point $z$, giving rise to a witness for the fact that $x \in \text{RWA}(G, A)$.
2. \( x \in \text{Cross}^+(P, \bar{P}, P') \). This case is illustrated in Figure 8. Let \( f \in \text{Adm}(x) \) and \( \delta_1, \delta_2 \) be the trajectory and the delays identified by the definition of \( \text{Cross}_4(P, \bar{P}, P') \). Let \( y = f(\delta_1), \ z = f(\delta_2) \), and \( t \) be an arbitrary point between them (i.e., \( t = f(\delta') \) for \( \delta' \in (\delta_1, \delta_2) \)). Let \( c = f(\delta_1) \), by applying Lemma 5 backwards from \( t \), we obtain that there exists \( \delta^* > 0 \) such that \( w \triangleq f(\delta_1) + \delta^* c \in \text{cl}(P') \cap \{ t \} \setminus \{ 0 \} \). Let \( w' \) be an intermediate point between \( w \) and \( t \).

Next, consider the points lying on the line segment between \( t \) and \( z \). Clearly, they belong to \( P' \). Hence, from each of them there is a witness that starts with a straight line segment (Lemma 11) and lingers in a patch in \( \mathbb{A} \). Let us pick a point \( u \) along the segment connecting \( t \) and \( z \), in such a way that all points between \( u \) (included) and \( t \) (excluded) have a witness that lingers in the same patch \( P'' \in \mathbb{A} \) (it may be \( P'' = P' \)). Let \( f' \) be such a witness for the point \( u \). In detail, \( f' \) starts with a straight line segment and lingers in \( P'' \). Formally, there exist a slope \( c \in F \) and a delay \( \delta' \) such that \( f'(\delta) = u + \delta c \) for all \( \delta \in [0, \delta'] \). Let \( v = f'(\delta') \). Let \( t' \) be an intermediate point on the line connecting \( t \) and \( u \).

In order to connect \( f \) to \( f' \), we apply Lemma 4 three times. First, to points \( x_0 = w, \ x_1 = t, \) and \( x_2 = w' \); then, to points \( x_0 = w', \ x_1 = t, \) and \( x_2 = t' \); finally, to points \( x_0 = t', \ x_1 = u, \) and \( x_2 = v \). In this way, we obtain three admissible trajectories \( f_1, f_2, f_3 \), with the following properties: \( f_1 \) and \( f_2 \) are contained in \( P' \) (with the possible exception of \( y = f_1(0) \)); \( f_3 \) is contained in \( P'' \) (with the possible exception of \( t = f_3(0) \)); \( f \) can be differentiably connected to \( f_1 \) in \( f(\delta_1) = y = f_1(0) \); \( f_1 \) can be differentiably connected to \( f_2 \) in \( w' \); \( f_2 \) can be differentiably connected to \( f_3 \) in \( t' \), and finally \( f_3 \) can be differentiably connected to \( f' \) in \( v \). The trajectory obtained by concatenating \( f \), the three trajectories \( f_1, f_2, f_3 \), and \( f' \) is a witness for \( x \).

7. CONCLUSIONS

In the paper we considered the problem of computing the set of points that can reach a given polyhedron while avoiding another one via a differentiable trajectory that is subject to a polyhedral differential inclusion. We have shown that previous solutions do not guarantee differentiability of the trajectories. We provided a precise formulation of the problem, showing that significant developments are needed to obtain the correct solution. This enabled us to devise the first exact algorithm in the literature to solve the problem.

As future work, we plan to implement the proposed algorithm using a library for polyhedra manipulation.

8. REFERENCES