2024 IEEE International Conference on Robotics and Automation (ICRA 2024)
May 13-17, 2024. Yokohama, Japan

A novel algorithmic approach to obtaining maneuverable control-invariant sets*

Prashant Solanki[1], Jasper J. van Beers[2], Anahita Jamshidnejad[3] and Coen C. de Visser[4]

***Abstract*— Ensuring safety in autonomous systems is essential as they become more integrated with modern society. One way to accomplish this is to identify and maintain a safe operating space. To this end, much effort has been devoted in the field of reachability analysis to obtaining control-invariant sets which ensure that a system inside of these sets can remain in these sets, and are thus essential for guaranteeing a system's safety. However, control invariance does not imply that a system can move from any state in the control-invariant set to any other state in the control-invariant set, within a given time horizon. In this paper, we develop an algorithm to obtain a control-invariant set that allows a given system to move from any state in the set to any other state in the set within a given time horizon without having to leave the set. We call this the 'maneuver set', $\mathscr{M}$. We substantiate the algorithm's efficacy through mathematical proof, affirming that the maneuver set obtained through the algorithm is indeed control-invariant. Furthermore, we prove that the system is indeed able to move from any state within this set to any other state in the set. To illustrate the use of our algorithm, we provide the numerical example of a Dubins car, utilising Hamilton-Jacobi-Bellman reachability analysis along with the proposed algorithm in order to obtain $\mathscr{M}$.**

I. INTRODUCTION

A. Motivation

The proliferation of automated systems in our daily lives underscores the growing importance of ensuring their safety. Indeed, as shown by [1], the predominant factor contributing to robot failures is loss-of-control. Furthermore, recent research by [2] has flagged a noteworthy correlation between the escalation of automation and robotics, and an increased incidence of accidents. These findings emphasize the need for better safety measures and strategies within these domains. Various engineering disciplines explore the safety concerns associated with such systems. One effective approach for providing safety guarantees is reachability analysis, which revolves around the conceptual framework of reachable sets. Reachability problems focus on identifying the set of states for which an attainable control policy exists, either to guide the system towards a specified state or to avoid particular states. Much effort has been devoted in the field of reachability analysis to obtain control-invariant sets. These sets ensure that, if the system is inside of these sets, there exists an attainable control input such that the system remains within the invariant set and are thus essential for guaranteeing a system's safety. However, control invariance does not imply that the system can move from any state in the control-invariant set to any other state in the control-invariant set, within the given time horizon. Thus, this paper is motivated by the aim of finding a set that is both control-invariant and allows the system to move from any state in the set to any other state in the set within the given time horizon. We call this set 'maneuver set', $\mathscr{M}$.

B. Related work

When addressing reachability problems, a variety of avenues have contributed useful approaches, often under different terminologies. Among these, the most prevalent term is 'capture basin' [3]. An alternative approach to obtain the capture basin is articulated within the framework of viability theory, as expounded in [4]. Another method for tackling the reachability problem involves formulating a value function incorporating optimal control principles, subsequently yielding a Hamilton-Jacobi-Bellman (HJB) equation. The solution to this equation is obtained through level set methods, wherein the zero level set of the HJB equation provides the solution to the reachability problem [5], [6], [7]. To address the challenges posed by the curse of dimensionality inherent to such grid-based approaches, innovative strategies have been explored, such as those based on Gaussian mixtures [8], convex optimization [9], particle filters [10], Lagrangian methods [11], and Monte Carlo simulations [12].

Apart from reachability analysis, another way for ensuring system safety involves the implicit design of a safety controller capable of modifying nominal control actions to preserve system integrity, as discussed in [13].

C. Contributions

The central contribution of this paper is the development of an algorithm for the computation of the maneuver set, $\mathscr{M}$. This set is a control-invariant set that allows the system to move from any state in the set to any other state in the set within the given time horizon. This set is constructed utilizing forward and backward reachable sets which are obtained through standard HJB reachability analysis. We prove that the maneuver set obtained through the application of the developed algorithm is indeed control invariant. Additionally, we further prove that the system is able to move from any state within $\mathscr{M}$ to any other state in $\mathscr{M}$, thereby affirming the

*This work was supported by a VIDI grant from the Dutch Research Council (NWO).

[1]PhD researcher at the Faculty of Aerospace Engineering, Delft University of Technology, 2629 HS Delft, The Netherlands. p.solanki@tudelft.nl

[2]PhD researcher at Faculty of Aerospace Engineering, Delft University of Technology, 2629 HS Delft, The Netherlands. J.J.vanBeers@tudelft.nl

[3]Assistant Professor at the Department of Control and Operations, Delft University of Technology, 2629 HS Delft, The Netherlands. A.Jamshidnejad@tudelft.nl

[4]Associate Professor at the Department of Control and Operations, Delft University of Technology, 2629 HS Delft, The Netherlands. C.C.deVisser@tudelft.nl

utility of the algorithm. To illustrate our findings, we provide the numerical example of a Dubins car. In this example, HJB reachability analysis is used to obtain the forward and backward reachable sets of the car from which the maneuver set is derived using the developed algorithm.

D. Organisation

Section II establishes the foundational context required and describes the problem statement. Section III introduces the algorithm and presents the accompanying mathematical proofs. Section IV delivers a concise introduction to HJB reachability analysis, while section V offers an introductory overview of the numerical example. Section VI presents the results and Section VII concludes the paper.

II. Setting and problem statement

Let the system be described by equation 1.

$$\frac{dx}{dt} = \dot{x} = f(x,u,d,\tau), \tau \in [t,T] \subseteq \mathbb{R}, t \geq 0, \\ x \in \mathbb{X} \subseteq \mathbb{R}^n, u \in \mathbb{U} \subseteq \mathbb{R}^m, d \in \mathbb{D} \subseteq \mathbb{R}^n \quad (1)$$

where x are the states of the system, $u(\cdot)$ is the input policy into the system, d is the disturbance to the system (input policy is also represented as u, due to space considerations). $\mathbb{X}, \mathbb{U}$ and $\mathbb{D}$ are continuous spaces (infinite sets), $\mathbb{R}$ is the set of real numbers and $\mathbb{F}$ is the set of all measurable functions. $\mathbb{U}_t^T$ is the set of all possible input policies in time horizon $[t,T]$ (whenever the time interval is obvious, $\mathbb{U}_t^T$ is replaced by $\mathbb{U}$ for the sake of readability). The system desrcibed by equation 1 is assumed to be locally Lipschitz continuous. $\mathbb{U}$ is compact and time invariant (for the given time interval), i.e., $\mathbb{U}_t^\tau = \mathbb{U}_{t+t_2}^{\tau+t_2}$. Furthermore, $\mathbb{U}_t^{T_1} \subseteq \mathbb{U}_t^{T_2}$ for $T_2 \geq T_1$. $\zeta_{x,t}^{u,d}(\tau)$ is the state of the system under control policy $u(\cdot)$, with initial state x and initial time t evaluated at time τ. It is further assumed that $\zeta_{x,t}^{u,d}(\tau) = \zeta_{x,t+t_2}^{u,d}(\tau + t_2)$ (this follows directly from the time-invariance of the system). The disturbance is assumed to be bounded, compact and time invariant (maximum and minimum disturbance is fixed).

In this paper, the disturbance, d, is a map, $d : \mathbb{U} \to \mathbb{D}$, i.e., player 2 (disturbance) is restricted to a strategy dependent upon player 1 (input), such that it always opposes the goals of player 1. Furthermore, it is assumed that player 2 can only draw from non-anticipative strategies (eq. (2)). This is a general assumption in robust control problems [14].

$$d \in \Lambda_t^T := \{\mathscr{N} : \mathbb{U}(t) \to \mathbb{D}(t) := u(\tau) = \hat{u}(\tau) \\ a.e.\ \tau \in [t,T]\} \quad (2) \\ \Rightarrow \mathscr{N}[u](\tau) = \mathscr{N}[\hat{u}](\tau)\ a.e.\ \tau \in [t,T]$$

This means that player 2 cannot produce a different strategy in response to player 1's strategy until player 1's strategy changes. Thus, player 2 cannot set their strategy based on the anticipated future strategy of player 1. However, in this setting player 2 has the advantage of deciding their strategy based on player 1 at every time instance. Thus, the disturbance has an instantaneous informational advantage. The reason for this is that, in robust problems, the worst case scenario is expected. The above assumptions guarantee the existence and uniqueness of the solution of the system equation (1).

The forward reachable set is the set of states for which there exists at least one control policy, for all possible disturbances, that will drive the system into the set from its initial set, $\mathscr{L}$, within the given time horizon. It is given by equation 3. This set is also called the robust forward reachable set.

$$V_{\text{FRT}}([t,T],\mathscr{L}) := \{y : \exists u \in \mathbb{U}_t^T, \forall d \in \mathbb{D}_t^T, \exists \tau \in [t,T], \\ x \in \mathscr{L}, \zeta_{x,t}^{u,d}(\tau) = y\} \quad (3)$$

The forced forward reachable set is the set of states for which there exists at least one possible disturbance, for all control policies, that will drive the system into the set from its initial set, $\mathscr{L}$, within the time horizon. It is given by equation 4.

$$V_{\text{FFRT}}([t,T],\mathscr{L}) := \{y : \forall u \in \mathbb{U}_t^T, \exists d \in \mathbb{D}_t^T, \exists \tau \in [t,T], \\ x \in \mathscr{L}, \zeta_{x,t}^{u,d}(\tau) = y\} \quad (4)$$

The backward reachable set is the set of all initial states from which there exists at least one control policy, for all possible disturbances, that will lead the system into the required set, $\mathscr{L}$, within the time horizon. It is given by equation 5. This set is also known as the robust backward reachable set.

$$V_{\text{BRT}}([t,T],\mathscr{L}) := \{x : \exists u \in \mathbb{U}_t^T, \forall d \in \mathbb{D}_t^T, \exists \tau \in [t,T], \\ \zeta_{x,t}^{u,d}(\tau) \in \mathscr{L}\} \quad (5)$$

The forced backward reachable set is the set of all the initial states from which there exists at least one possible disturbance, for all control policies, that will lead the system into the required set, $\mathscr{L}$, within the time horizon. It is given by equation 6. This set is also known as the avoid backward reachable set [7].

$$V_{\text{FBRT}}([t,T],\mathscr{L}) := \{x : \forall u \in \mathbb{U}_t^T, \exists d \in \mathbb{D}_t^T, \exists \tau \in [t,T], \\ \zeta_{x,t}^{u,d}(\tau) \in \mathscr{L}\} \quad (6)$$

The control invariant set is defined as the set of states such that, if the system is inside of the control invariant set, there exists a control policy such that the system stays inside of the control invariant set for the given time horizon. Equation 7 defines the control invariant set, $V_{\text{cinv}}([t,T])$. The union of all control invariant sets for the given time horizon is called the control invariant kernel and is denoted by $K_{\text{cinv}}([t,T])$, i.e., the control invariant kernel is the biggest control invariant set. It is also referred to as robust control invariant set and robust control invariant kernel, respectively.

$$V_{\text{cinv}}([t,T]) := \{x : \exists u \in \mathbb{U}_t^T, \forall d \in \mathbb{D}_t^T, \\ \forall \tau \in [t,T], x \in V_{\text{cinv}}([t,T]), \zeta_{x,t}^{u,d}(\tau) \in V_{\text{cinv}}([t,T])\} \quad (7)$$

The intersection of forward and backward reachable set (often called the safe set in literature [15],[16],[17]) is shown in equation 8. In this paper we will refer to this set as intersection set.

$$V_{\text{int}}([t,T],\mathscr{L}) = V_{\text{BRT}}([t,T],\mathscr{L}) \cap V_{\text{FRT}}([t,T],\mathscr{L}) \quad (8)$$

In this paper we define a set called maneuver set. It is a

control invariant set in which the system can travel form any state in the maneuver set to any other state in the maneuver set within the given time horizon. The set is denoted as $\mathscr{M}([t,T])$.

We also define a trajectory set. Given a control policy (u), a time horizon ($[t,T]$), and an initial state (x), this is the set of all the states that the system transitions to from the initial state in the time horizon under the control policy. We represent this set as $\{\zeta_{x,t}^{u,d}(T)\}$. One must note that since disturbance d is dependent on the control input (in a robust sense) the trajectory set is deterministic in nature.

The definitions of the sets provided above are valid under the assumption that the control policy set ($\mathbb{U}_t^T$) and the disturbance set ($\mathbb{D}_t^T$) are compact in nature, i.e., they are bounded and closed sets. The control set is usually assumed to be compact, which is true for the systems of interest (i.e., physical systems). However, the disturbance set can be bounded or unbounded based on the environment.

III. Main Contribution - The Maneuver Set

The algorithm developed in this paper (algorithm 1) aims to find a control-invariant set in which the system can travel from any state to any state within a given time horizon without leaving the set. Algorithm 1, in essence, utilises the forward and backward reachable sets of an initial set, $\mathscr{L}$ and obtains their intersection. Then it computes the complement of this intersection and finds the forced backward reachable set of this complement. It then subtracts this forced backward reachable set from the intersection, resulting in the set with the desired properties, i.e., the maneuver set (set $\mathscr{M}$).

Algorithm 1 An algorithm to obtain maneuver set ($\mathscr{M}$)

Require: $V_{\text{BRT}}([t,T],\mathscr{L}), V_{\text{FRT}}([t,T],\mathscr{L})$
$V_{\text{int}}([t,T],\mathscr{L}) = S \leftarrow V_{\text{BRT}}([t,T],\mathscr{L}) \cap V_{\text{FRT}}([t,T],\mathscr{L})$
Obtain $\overline{S} = \mathbb{X} \setminus S$
$Q \leftarrow V_{\text{FBRT}}([t,T],\overline{S})$
$\mathscr{M} = S \setminus Q$

The first part of the algorithm to obtain the maneuver set ($\mathscr{M}$) involves taking the intersection of the forward and backward reachable sets of an initial set, $\mathscr{L}$ and thus obtaining the intersection set, S ($V_{\text{int}}([t,T],\mathscr{L})$). As proven in lemma 1, within the set S, the system can transition from any state to any state. That is because any state inside of the intersection set is also part of set $\mathscr{L}$'s backward reachable set. Per definition this means that within the time horizon 0 to T the system can reach set $\mathscr{L}$. Furthermore, as per definition $\mathscr{L}$ is a subset of its own forward reachable set. Thus, the system can start from any state within $\mathscr{L}$ and can reach any state in the forward reachable set within the time horizon 0 to T.

Lemma 1: The system can transition from any state in the $V_{\text{int}}([0,T],\mathscr{L})$ to any other state in $V_{\text{int}}([0,T],\mathscr{L})$ within the time horizon of [0,2T].

Proof : Let $x, x_1 \in V_{\text{int}}([0,T],\mathscr{L})$

$$\text{Since } x \in V_{\text{int}}([0,T],\mathscr{L}) \Rightarrow x \in V_{\text{BRT}}([0,T],\mathscr{L}) \Rightarrow$$
$$\exists u \in \mathbb{U}_0^T, \forall d \in \mathbb{D}_0^T, \exists \tau \in [0,T], \text{ s.t. } \zeta_{x,0}^{u,d}(\tau) = x_{\mathscr{L}} \in \mathscr{L}$$

Since the system is time invariant

$$V_{\text{FRT}}([0,T],\mathscr{L}) = V_{\text{FRT}}([\tau,T+\tau],\mathscr{L})$$
$$\Rightarrow x' \in V_{\text{int}}([0,T],\mathscr{L}) \Rightarrow x' \in V_{\text{FRT}}([\tau,T+\tau],\mathscr{L}) \Rightarrow$$
$$\exists u' \in \mathbb{U}_\tau^{T+\tau}, \forall d' \in \mathbb{D}_\tau^{T+\tau}, \exists \tau' \in [\tau,T+\tau],$$
$$x_{\mathscr{L}} \in \mathscr{L}, \zeta_{x_{\mathscr{L}},\tau}^{u',d'}(\tau') = x'$$
$$\Rightarrow \exists u'' \in \mathbb{U}_0^{2T}, \forall d'' \in \mathbb{D}_0^{2T}, \exists \tau'' \in [0,2T] \text{ s.t.}$$
$$x, x' \in V_{\text{int}}([0,T],\mathscr{L}), \zeta_{x,0}^{u'',d''}(\tau'') = x'$$

However, this does not imply that the intersection set is control-invariant, as depicted in figure 1. It can be observed that the system at any state within the set S can transition to any state in $\mathscr{L}$ (as $\forall x \in S \Rightarrow x \in V_{\text{BRT}}([t,T],\mathscr{L})$) but the only way to do so might be by leaving set S, as illustrated by the red trajectory in figure 1. In contrast, for the blue dot there exists a control, and thus a trajectory, which leads the system into set $\mathscr{L}$ while ensuring that the complete trajectory stays inside the intersection set during the given time frame.

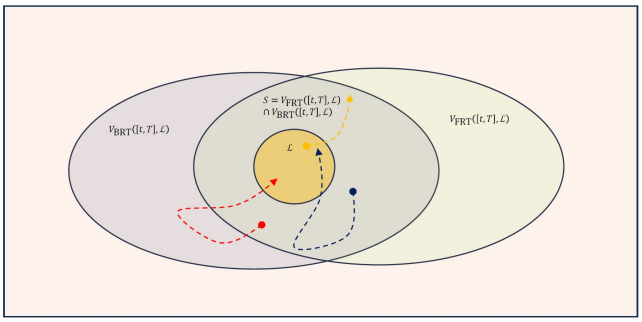

Fig. 1. Illustration to provide a visual understanding of Lemma 1: (—),(—) and (—) represent the trajectory set.

Lemma 2 proves that set $\mathscr{M}$ is control-invariant. After finding the intersection of the forward and backward reachable set of set $\mathscr{L}$, we now want to find all the states in this intersection that force the system to leave the intersection in order to reach set $\mathscr{L}$, similar to the red trajectory in figure 1. These states are found by using the complement of the intersection set (represented by $\overline{S}$) and finding the forced backward reachable set of this complement, Q ($V_{\text{FBRT}}([t,T],\overline{S})$). Q consists of all the states that force the system into the complement of the intersection set $\overline{S}$ (which by definition is outside of the intersection set). Thus, we are provided with the set of states that we want to eliminate from the intersection set. These states are subsequently removed from the intersection set.

If we now take any state in this transformed intersection set (i.e. $\mathscr{M}$), we can be sure that the system will never leave the original intersection set since all states that would force it to leave have been eliminated from it. We also prove that the system will stay inside set $\mathscr{M}$ at all times. This is

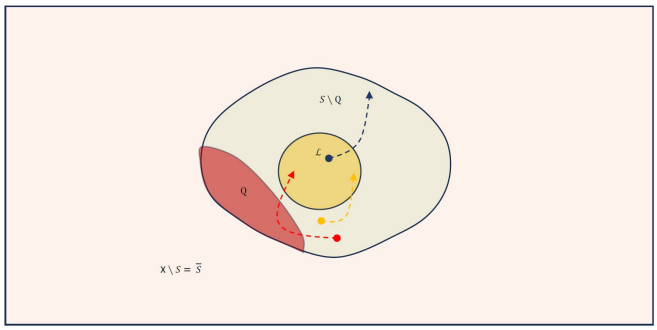

Fig. 2. Illustration to provide a visual understanding of Lemma 2: (—),(—) and (—) represent the trajectory set .

because any state inside set $\mathscr{M}$ is also a state in the backward reachable set of set $\mathscr{L}$. It is not possible that there exists a trajectory to $\mathscr{L}$ (e.g., the red trajectory in figure 2) that exits set $\mathscr{M}$ and crosses any state we have removed from the intersection set (illustrated by area Q in figure 2).

That is because if such a trajectory existed, it would imply that there is a direct trajectory from a state in Q to $\mathscr{L}$ which does not force the system outside of the intersection set. But if that was the case, this state would not have been part of Q in the first place. Therefore, the set $\mathscr{M}$ is control-invariant.

Lemma 2: The set $\mathscr{M}$ is a control invariant.

Proof: Part I

Since $S \cup \overline{S} = \mathbb{X}$

$\Rightarrow Q = V_{\text{FBRT}}([t,T],\overline{S}) \subseteq S$

Part II

Let $x \in \mathscr{M} \Rightarrow x \in S \wedge x \notin Q$

where $\wedge$ is the 'AND' operation

if $x \in Q = V_{\text{FBRT}}([t,T],\overline{S}) \Rightarrow \forall u \in \mathbb{U}_t^T, \exists d \in \mathbb{D}_t^T,$

$\exists \tau \in [t,T],$ s.t. $\zeta_{x,t}^{u,d}(\tau) \in \overline{S}$

Since $x \notin Q \Rightarrow \exists u \in \mathbb{U}_t^T, \forall d \in \mathbb{D}_t^T,$

$\forall \tau \in [t,T],$ s.t. $\zeta_{x,t}^{u,d}(\tau) \in S$

$x \in \mathscr{M} = S \setminus Q \Rightarrow \exists u \in \mathbb{U}_t^T, \forall d \in \mathbb{D}_t^T,$

$\forall \tau \in [t,T],$ s.t. $\zeta_{x,t}^{u,d}(\tau) \in S$

Part III

Let $x' \in \mathscr{M} \Rightarrow x' \in S \Rightarrow x' \in V_{\text{BRT}}([t,T],\mathscr{L}) \cap$

$V_{\text{FRT}}([t,T],\mathscr{L}) \Rightarrow x' \in V_{\text{BRT}}([t,T],\mathscr{L})$

$\Rightarrow \exists u' \in \mathbb{U}_t^T, \forall d \in \mathbb{D}_t^T, \exists \tau' \in [t,T]$ s.t. $\zeta_{x',t}^{u',d}(\tau') \in \mathscr{L}$

It is evident from definition of the set S that $\mathscr{L} \subseteq S$

$\Rightarrow \exists u' \in \mathbb{U}_t^T, \forall d \in \mathbb{D}_t^T, \exists \tau' \in [t,T]$ s.t. $\zeta_{x',t}^{u',d}(\tau') \in S$

Let $\{\zeta_{x',t}^{u',d}(\tau')\}$ be the trajectory set then

using part II $\{\zeta_{x',t}^{u',d}(\tau')\} \subseteq S$

Part IV

Claim: $Q \cap \{\zeta_{x',t}^{u',d}(\tau')\} = \phi$, Where ϕ is empty set

Let the claim be false $\Rightarrow Q \cap \{\zeta_{x',t}^{u',d}(\tau')\} \neq \phi$

$\Rightarrow \exists \tau'' \in [t,\tau']$ s.t. $\zeta_{x',t}^{u',d}(\tau'') = x'' \in Q \cap \{\zeta_{x',t}^{u',d}(\tau')\}$

Since $x'' \in \{\zeta_{x',t}^{u',d}(\tau')\} \Rightarrow \exists u' \in \mathbb{U}_t^T, \forall d \in \mathbb{D}_t^T,$

$\forall \tau''' \in [\tau'',\tau']$ s.t. $\zeta_{x'',\tau''}^{u',d}(\tau''') \in S$

Since $x'' \in Q \Rightarrow \forall u \in \mathbb{U}_t^T, \exists d \in \mathbb{D}_t^T,$

$\exists \tau \in [t,T],$ s.t. $\zeta_{x,t}^{u,d}(\tau) \in \overline{S}$

This is a contradiction; thus the claim is true

and by using part II, III and IV

$x' \in \mathscr{M} \Rightarrow \exists u' \in \mathbb{U}_t^T, \forall d \in \mathbb{D}_t^T, \forall \tau' \in [t,T]$

s.t. $\zeta_{x',t}^{u',d}(\tau') \in S \setminus Q$

Lemma 3 proves that within set $\mathscr{M}$ the system can travel from any state to any state. $\mathscr{M}$ is a subset of the intersection set, for which lemma 1 has proven that the system can travel from any state to any state. Using the same argument we can show that the system can travel from any state to any state in set $\mathscr{M}$.

As illustrated by figure 3: From any state in set $\mathscr{M}$ the system can take a trajectory to $\mathscr{L}$ (yellow trajectory), and from $\mathscr{L}$ the system can go to any state within $\mathscr{M}$ (blue trajectory).

Lemma 3: The system can transition from any state in $\mathscr{M}$ to any other state in $\mathscr{M}$, in time horizon $[0,2T]$.

Proof: Let $x \in \mathscr{M}$

Let $x \in \mathscr{M} \Rightarrow x \in S \Rightarrow x \in$

$V_{\text{BRT}}([0,T],\mathscr{L}) \cap V_{\text{FRT}}([0,T],\mathscr{L})$

$\Rightarrow x \in V_{\text{BRT}}([0,T],\mathscr{L}) \Rightarrow \exists u \in \mathbb{U}, \forall d \in \mathbb{D}, \exists \tau \in [0,T]$

s.t. $\zeta_{x,0}^{u,d}(\tau) = x' \in \mathscr{L}$

Since $\mathscr{L} \subseteq S \Rightarrow x' \in S \Rightarrow x' \in V_{\text{FRT}}([0,T],\mathscr{L})$

$\Rightarrow \exists u' \in \mathbb{U}, \forall d \in \mathbb{D}, \exists \tau' \in [0,T]$ s.t. $\zeta_{x',0}^{u',d}(\tau') = x''$

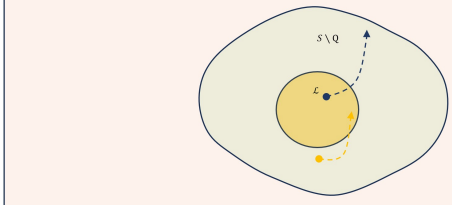

Fig. 3. Illustration to provide a visual understanding of Lemma 3: (—) and (—) represents the trajectory set and $S \setminus Q = \mathscr{M}$.

Since system is assumed to be time invariant

$$\Rightarrow \exists u' \in \mathbb{U}, \forall d \in \mathbb{D}, \exists \tau' \in [T, 2T] \text{ s.t. } \zeta_{x',T}^{u',d}(\tau') = x''$$

$$\Rightarrow \exists u'' \in \mathbb{U}, \forall d \in \mathbb{D}, \exists \tau'' \in [0, 2T], x, x'' \in \mathscr{M}$$
$$\text{s.t. } \zeta_{x,0}^{u',d}(\tau') = x''$$

IV. Hamilton Jacobi Bellman reachability analysis

In this subsection a short overview of Hamilton-Jacobi-Bellman (HJB) reachability analysis is provided. This technique is used to obtain the forward/backward reachable set pertaining to both reach and avoid scenarios [18], [19], [20], [21]. A cost function is designed as shown in equation 9.

$$J(x,t,u) = \int_t^T c(x(\tau), u(\tau)) d\tau + l(x(T)) \tag{9}$$

Then an optimal control problem is formulated such that the cost function is minimised with the system dynamics as one of the constraints as shown in equation (10).

$$V(x(t),t) = \inf_u [J(x,t,u)] \tag{10}$$
$$\text{subject to } \dot{x} = f(x(\tau), u(\tau)), \forall \tau \in [t,T]$$
$$u(\tau) \in \mathbb{U}_t^T$$

This optimal control problem is solved using dynamic programming, giving rise to a partial differential equation (PDE) called HJB PDE for the continuous case, or a recursive update equation called Bellman backup/equation in the case of discrete systems. The zero level set of the solution of this PDE provides us with the set of interest. This method further produces a control law or a controller that can keep the system in the set of interest. We obtain different value functions for different sets of interest, which correspond to different HJB PDE [22]. For backward reachable sets the value function is given by equation 11 and the corresponding PDE is given by equation 12

$$V_{\text{BRT}}([t,T], \mathscr{L}) = \inf_u \sup_d \min_{\tau \in t,T} l(\zeta_{x,t}^{u,d}(\tau)) \tag{11}$$

$$min\{l(x,t) - V(x,t), D_t V + \inf_u \sup_d D_x V \cdot f(x,u)\} = 0 \tag{12}$$

The optimal control at any given time and state is given by equation 13

$$u^*(x,t) = \arg\inf_u \sup_d [D_x V \cdot f(x(t), u(t))] \tag{13}$$

For forced backward reachable sets the value function is given by equation 14 and the corresponding PDE is given by equation 15

$$V_{\text{FBRT}}([t,T], \mathscr{L}) = \sup_u \inf_d \min_{\tau \in t,T} l(\zeta_{x,t}^{u,d}(\tau)) \tag{14}$$

$$min\{l(x,t) - V(x,t), D_t V + \sup_u \inf_d D_x V \cdot f(x,u)\} = 0 \tag{15}$$

The optimal control at any given time and state is given by equation 16

$$u^*(x,t) = \arg\sup_u \inf_d [D_x V \cdot f(x(t), u(t))] \tag{16}$$

For forward reachable sets the value function is given by equation 17 and the corresponding PDE by equation 18.

$$V_{\text{FRT}}([t,T], \mathscr{L}) = \inf_u \sup_d \max_{\tau \in t,T} l(\zeta_{x,t}^{u,d}(\tau)) \tag{17}$$

$$max\{l(x,t) - V(x,t), D_t V - \inf_u \sup_d D_x V \cdot f(x,u)\} = 0 \tag{18}$$

The optimal control at any given time and state is given by equation 19

$$u^*(x,t) = \arg\inf_u \sup_d [-D_x V \cdot f(x(t), u(t))] \tag{19}$$

The obtained HJB PDE is solved using numerical methods. One of the most common methods is the level set method [23], [24]. There are also toolboxes available that are specifically created to solve HJB PDE for reachability analysis.

V. Numerical example: Dubins car

To demonstrate the theoretical results of the preceding sections, we employ the Dubins car with a constant speed v as the system model, shown in equation 20.

$$\begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{\theta} \end{bmatrix} = \begin{bmatrix} v\cos(\theta) \\ v\sin(\theta) \\ \omega \end{bmatrix} + \begin{bmatrix} d_x \\ d_y \\ d_\theta \end{bmatrix}, \omega \in [-1,1] \tag{20}$$

where x is the position along the x-axis, y is the position along the y-axis, θ is the turn angle, ω is the input to the system and v is the constant velocity of the car which is assumed to be 1 m/s. It is assumed that ω is bounded between $[-1,1]$. Furthermore, the disturbance is also assumed to be bounded with $d_x \in [-0.1, 0.1]$, $d_y \in [-0.1, 0.1]$ and $d_\theta \in [-0.1, 0.1]$ We follow the steps of the algorithm as explained in section III.

VI. Results and discussion

To obtain the forward and backward reachable sets, a cylinder with a radius of 1 centred at origin was chosen as the initial set $\mathscr{L}$. Physically this initialisation means that the Dubins car could be situated at any state within a circle of radius 1 with an initial orientation of any angle between 0 and 360. Using the level set method and a customised version of the toolbox [25], equation 18 is solved to compute the forward reachable set of the initial set $\mathscr{L}$. Figure 4 shows the outer contour of the forward reachable set ($V_{\text{BRT}}([t,T], \mathscr{L})$) of the system represented by equation 20 for a time horizon of 5 seconds in green, while the outer contour of initial set ($\mathscr{L}$) is depicted in blue. The x-axis and y-axis of the figure represent distances in metres. The z-axis represents the turn angle or yaw angle of the system in radians.

Using the same toolbox, the backward reachable set of the initial set $\mathscr{L}$ is found through equation 12. Figure 5 shows the outer contour of the backward reachable set ($V_{\text{BRT}}([t,T], \mathscr{L})$) of the system represented by equation 20 for a time horizon of 5 seconds in green colour, while the outer contour of initial set ($\mathscr{L}$) is depicted using blue colour. The x-axis and y-axis of the figure represent the distances travelled in metres. The z-axis represents the turn angle or yaw angle of the system in radians.

Using the forward and backward reachable sets as inputs into the algorithm developed in this paper and once again

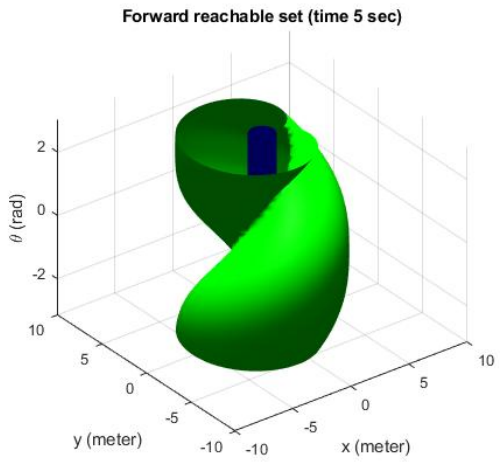

Fig. 4. Outer contour of the forward reachable set denoted by colour (—) and initial set denoted by colour (—)

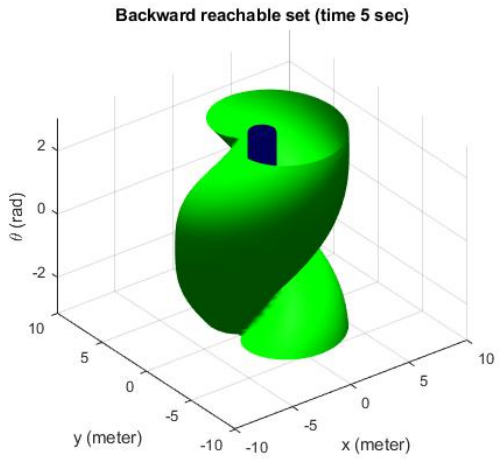

Fig. 5. Outer contour of the backward reachable set denoted by colour (—) and initial set denoted by colour (—)

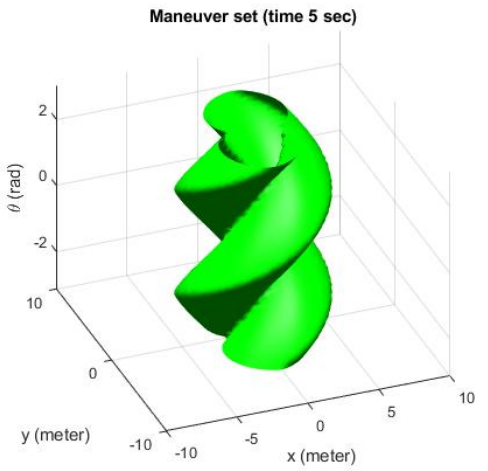

Fig. 6. Outer contour of the maneuver set denoted by colour (—)

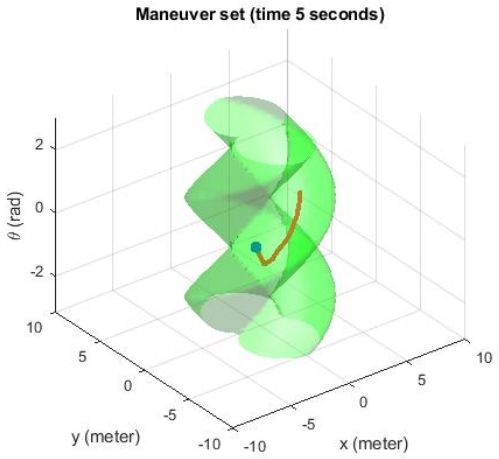

Fig. 7. Outer contour of the maneuver set denoted by colour (—), initial state denoted by colour (—) and the trajectory taken by the system denoted by colour (—)

using the modified toolbox, we arrive at the maneuver set $\mathscr{M}$. Figure 6 shows the outer contour of the maneuver set ($\mathscr{M}$) of the system represented by equation 20 for a time horizon of 5 seconds in green colour. The x-axis and y-axis of the figure represent the distances travelled in metres. The z-axis represents the turn angle or yaw angle of the system in radians.

To illustrate that the system is able to stay within the maneuver set, we chose a random state within the maneuver set and show that the system is able to stay inside it for 5 seconds. This serves as an illustration for the set's control invariance. Figure 7 shows the outer contour of the maneuver set ($\mathscr{M}$) of the system represented by equation 20 for a time horizon of 5 seconds in green colour, an initial condition of the system in blue colour and the trajectory followed by the system in red colour. The x-axis and y-axis of the figure represent the distances travelled in metres. The z-axis represents the turn angle or yaw angle of the system in radians.

VII. Conclusion

To ensure the safety of automated systems it is essential that they are aware of the region in the state space where they have the control authority to move safely, and the capability to stay within that region. We have derived a definition of such a set, called the maneuver set, which can be computed from forward and backward reachable sets. We illustrated the computation of the set through an example. In future we would like to expand the concept of the maneuver set into the probabilistic domain to obtain probabilistic control-invariant sets that guarantee the system to move from one state to another state with a certain probability.

References

[1] J. Carlson, R. R. Murphy, and A. Nelson, "Follow-up analysis of mobile robot failures," in *IEEE International Conference on Robotics and Automation, 2004. Proceedings. ICRA'04. 2004*, vol. 5, pp. 4987–4994, IEEE, 2004.

[2] S. Yang, Y. Zhong, D. Feng, R. Y. M. Li, X.-F. Shao, and W. Liu, "Robot application and occupational injuries: are robots necessarily safer?," *Safety science*, vol. 147, p. 105623, 2022.

[3] J.-P. Aubin and H. Frankowska, "Viability kernel of control systems," in *Nonlinear synthesis*, pp. 12–33, Springer, 1991.

[4] P. Cardaliaguet, "A differential game with two players and one target," *SIAM Journal on Control and Optimization*, vol. 34, no. 4, pp. 1441–1460, 1996.

[5] J. Lygeros, "On reachability and minimum cost optimal control," *Automatica*, vol. 40, no. 6, pp. 917–927, 2004.

[6] S. Bansal, M. Chen, S. Herbert, and C. J. Tomlin, "Hamilton-jacobi reachability: A brief overview and recent advances," in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pp. 2242–2253, IEEE, 2017.

[7] S. L. Herbert, M. Chen, S. Han, S. Bansal, J. F. Fisac, and C. J. Tomlin, "Fastrack: A modular framework for fast and guaranteed safe motion planning," in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pp. 1517–1522, IEEE, 2017.

[8] N. Kariotoglou, K. Margellos, and J. Lygeros, "On the computational complexity and generalization properties of multi-stage and stage-wise coupled scenario programs," *Systems & Control Letters*, vol. 94, pp. 63–69, 2016.

[9] K. Lesser, M. Oishi, and R. S. Erwin, "Stochastic reachability for control of spacecraft relative motion," in *52nd IEEE Conference on Decision and Control*, pp. 4705–4712, IEEE, 2013.

[10] G. Manganini, M. Pirotta, M. Restelli, L. Piroddi, and M. Prandini, "Policy search for the optimal control of markov decision processes: A novel particle-based iterative scheme," *IEEE transactions on cybernetics*, vol. 46, no. 11, pp. 2643–2655, 2015.

[11] J. N. Maidens, S. Kaynama, I. M. Mitchell, M. M. Oishi, and G. A. Dumont, "Lagrangian methods for approximating the viability kernel in high-dimensional systems," *Automatica*, vol. 49, no. 7, pp. 2017–2029, 2013.

[12] S. Sun and C. C. de Visser, "Quadrotor safe flight envelope prediction in the high-speed regime: A monte-carlo approach," in *AIAA Scitech 2019 Forum*, p. 0948, 2019.

[13] K. P. Wabersich and M. N. Zeilinger, "Linear model predictive safety certification for learning-based control," in *2018 IEEE Conference on Decision and Control (CDC)*, pp. 7130–7135, IEEE, 2018.

[14] S. L. Herbert, *Safe real-world autonomy in uncertain and unstructured environments*. University of California, Berkeley, 2020.

[15] E. Van Oort, Q. Chu, and J. Mulder, "Maneuver envelope determination through reachability analysis," in *Advances in Aerospace Guidance, Navigation and Control: Selected Papers of the 1st CEAS Specialist Conference on Guidance, Navigation and Control*, pp. 91–102, Springer, 2011.

[16] T. Lombaerts, S. Schuet, K. Wheeler, D. M. Acosta, and J. Kaneshige, "Safe maneuvering envelope estimation based on a physical approach," in *Aiaa guidance, navigation, and control (gnc) conference*, p. 4618, 2013.

[17] S. Schuet, T. Lombaerts, D. Acosta, K. Wheeler, and J. Kaneshige, "An adaptive nonlinear aircraft maneuvering envelope estimation approach for online applications," in *Aiaa guidance, navigation, and control conference*, p. 0268, 2014.

[18] M. Chen, S. Herbert, and C. J. Tomlin, "Exact and efficient hamilton-jacobi guaranteed safety analysis via system decomposition," in *2017 IEEE International Conference on Robotics and Automation (ICRA)*, pp. 87–92, IEEE, 2017.

[19] M. Chen, S. L. Herbert, M. S. Vashishtha, S. Bansal, and C. J. Tomlin, "Decomposition of reachable sets and tubes for a class of nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 63, no. 11, pp. 3675–3688, 2018.

[20] M. Chen, S. L. Herbert, H. Hu, Y. Pu, J. F. Fisac, S. Bansal, S. Han, and C. J. Tomlin, "Fastrack: a modular framework for real-time motion planning and guaranteed safe tracking," *IEEE Transactions on Automatic Control*, vol. 66, no. 12, pp. 5861–5876, 2021.

[21] J. J. Choi, D. Lee, K. Sreenath, C. J. Tomlin, and S. L. Herbert, "Robust control barrier–value functions for safety-critical control," in *2021 60th IEEE Conference on Decision and Control (CDC)*, pp. 6814–6821, IEEE, 2021.

[22] S. L. Herbert, *Safe real-world autonomy in uncertain and unstructured environments*. University of California, Berkeley, 2020.

[23] J. A. Sethian, *Level set methods and fast marching methods: evolving interfaces in computational geometry, fluid mechanics, computer vision, and materials science*, vol. 3. Cambridge university press, 1999.

[24] S. Osher and R. P. Fedkiw, *Level set methods and dynamic implicit surfaces*, vol. 1. Springer New York, 2005.

[25] I. M. Mitchell and J. A. Templeton, "A toolbox of hamilton-jacobi solvers for analysis of nondeterministic continuous and hybrid systems," in *Hybrid Systems: Computation and Control: 8th International Workshop, HSCC 2005, Zurich, Switzerland, March 9-11, 2005. Proceedings 8*, pp. 480–494, Springer, 2005.