Data-Driven Hamiltonian for Direct Construction of Safe Set from Trajectory Data

Jason J. Choi*[1], Christopher A. Strong*[1], Koushil Sreenath[1], Namhoon Cho†[2], and Claire J. Tomlin†[1]

***Abstract*— In continuous-time optimal control, evaluating the Hamiltonian requires solving a constrained optimization problem using the system's dynamics model. Hamilton-Jacobi reachability analysis for safety verification has demonstrated practical utility only when efficient evaluation of the Hamiltonian over a large state-time grid is possible. In this study, we introduce the concept of a data-driven Hamiltonian (DDH), which circumvents the need for an explicit dynamics model by relying only on mild prior knowledge (e.g., Lipschitz constants), thus enabling the construction of reachable sets directly from trajectory data. Recognizing that the Hamiltonian is the optimal inner product between a given costate and realizable state velocities, the DDH estimates the Hamiltonian using the worst-case realization of the velocity field based on the observed state trajectory data. This formulation ensures a conservative approximation of the true Hamiltonian for uncertain dynamics. The reachable set computed based on the DDH is also ensured to be a conservative approximation of the true reachable set. Next, we propose a data-efficient safe experiment framework for gradual expansion of safe sets using the DDH. This is achieved by iteratively conducting experiments within the computed data-driven safe set and updating the set using newly collected trajectory data. To demonstrate the capabilities of our approach, we showcase its effectiveness in safe flight envelope expansion for a tiltrotor vehicle transitioning from near-hover to forward flight.**

I. Introduction

Data-driven safety verification is needed to ensure the safety of various real-world systems that involve uncertain dynamics. Such uncertainty, which may be impossible to model or require extensive modeling efforts, can result from various sources—complex aerodynamics in unconventional aircraft, robot manipulation of non-rigid objects, learning-enabled components in an autonomy stack, interaction with unstructured environments, and many others.

Hamilton-Jacobi (HJ) reachability, rooted in model-based optimal control, provides a rigorous and flexible framework for verifying safety by computing the maximal safe set within constraints, as well as an associated safe policy [1]. However, its practical applicability is limited by the need to evaluate the Hamiltonian, which is the optimal directional derivative of the value function along the dynamics. Evaluating the Hamiltonian involves solving a constrained optimization problem in the control input space. Consequently, both the lack of an accurate dynamics model as well as any computational challenges in the optimization can hinder the implementation of HJ reachability analysis in practice.

Existing data-driven approaches address these challenges *indirectly* by using supervised learning to approximate components needed to evaluate the Hamiltonian. For instance, [2] employs Gaussian processes to learn the dynamics, while [3] fits a neural network to approximate the Hamiltonian. However, these methods rely heavily on the quality of the learned model and may introduce inefficiencies due to misalignment between model learning and safety verification. Alternative data-driven methods outside the HJ framework primarily focus on forward reachability [4], [5], [6], [7].

We propose a new data-driven approach by approximating the Hamiltonian used in HJ reachability *directly* from data. The constrained optimization involved in computing the original Hamiltonian is replaced with an efficient data-enabled approximation, which computes its best approximation under the worst-case realization of the dynamics inferred from the data. Using this approximate Hamiltonian in HJ reachability allows the safe set to be computed directly from trajectory data without any intermediate supervised learning step.

Our main contributions are summarized below:

- We propose the *data-driven Hamiltonian* (DDH), a novel concept enabling *direct* data-driven reachability analysis for uncertain dynamics under mild assumptions of knowledge of the system's Lipschitz constants.
- We prove that using this DDH in HJ reachability computations guarantees a conservative approximation of the true safe set.
- We present a safe set expansion framework built upon the DDH-based reachability method, which can iteratively update a data-driven safe set while running experiments that safely collect more data.
- We demonstrate the effectiveness of our approach in safe longitudinal flight envelope expansion for a tiltrotor vehicle transitioning from near-hover to forward flight.

Notations. The norm $\|\cdot\|$ being used is the l_2 norm, and $|\cdot|$ denotes an absolute value. An l_2 hypersphere centered at the origin with radius r will be notated as $\mathrm{B}(r) = \{x \mid \|x\| \leq r\}$. A hyperrectangle centered at the origin with element-wise radii $r \in \mathbb{R}^{n_x}$ will be denoted as $\mathrm{Rect}(r) = \{x \mid |x_j| \leq r_j, \forall j = 1, \cdots, n_x\}$. The symbol $\oplus$ indicates the Minkowski sum of two sets. The superscript i denotes the index of a data point and the subscript j denotes the j-th element of a vector unless noted otherwise.

This is the extended version of the article.

* Equal first authorship. † Equal advising.

[1]Jason J. Choi, Christopher A. Strong, Koushil Sreenath, and Claire J. Tomlin are with the University of California, Berkeley, CA 94720 USA. jason.choi, christopher_strong@berkeley.edu

[2]Namhoon Cho is with the Centre for Assured and Connected Autonomy at Cranfield University, United Kingdom.

This research is supported in part by the NASA ULI on Safe Aviation Autonomy, NSF Safe Learning-Enabled Systems, and the ONR LEARN projects. The work of Jason J. Choi received the support of a fellowship from Kwanjeong Educational Foundation, Korea.

II. Problem Formulation & Background

A. Problem Formulation

We consider nonlinear system dynamics

$$\dot{\boldsymbol{x}}(s) = f(\boldsymbol{x}(s), \boldsymbol{u}(s)) \text{ for } s \in [-t, 0], \quad \boldsymbol{x}(-t) = x, \tag{1}$$

with state $\boldsymbol{x}(s) \in \mathbb{R}^{n_x}$, control $\boldsymbol{u}(s) \in U \subset \mathbb{R}^{n_u}$, and initial state x at time $-t$, where $t > 0$ and U is the control input set. The vector field f is assumed to be Lipschitz continuous in the state, which is required for the forward completeness of the trajectory [8]. We consider various forms of Lipschitz continuity:

(i) uniform Lipschitz constant L^x, satisfying

$$\|f(x,u) - f(x',u)\| \leq L^x \|x - x'\|, \tag{2}$$

(ii) input-element-wise constant vector L^{in} satisfying

$$\|f(x,u) - f(x',u)\| \leq \sum_{j=1}^{n_x} L_j^{\text{in}} |x_j - x'_j| \tag{3}$$

(iii) output-element-wise constant vector L^{out} satisfying for $i = 1, \cdots, n_x$,

$$|f_i(x,u) - f_i(x',u)| \leq L_i^{\text{out}} \|x - x'\| \tag{4}$$

(iv) $n_x \times n_x$ sensitivity matrix L^{io} satisfying for $i = 1, \cdots, n_x$,

$$|f_i(x,u) - f_i(x',u)| \leq \sum_{j=1}^{n_x} L_{ij}^{\text{io}} |x_j - x'_j| \tag{5}$$

for all $x, x' \in \mathcal{X}, u \in \mathcal{U}$.

While the dynamics f itself is deemed uncertain and unknown, we assume that (i) a dataset of trajectories from this uncertain system is given as $\mathcal{D} = \{(x^i, u^i, v^i)\}_{i=1}^N$, where $v^i := f(x^i, u^i)$ denotes "state velocity", and (ii) we know at least one of the Lipschitz constants of f above. The dataset is collected from experiments, where the state, control, and state velocity are sampled at various time steps of the trajectories of (1). The Lipschitz constants may come from prior knowledge or can be estimated directly from the dataset $\mathcal{D}$. While access to a valid constant indicates that our method is not completely model-free and requires basic system knowledge, the required modeling effort is significantly less than accurately characterizing the full dynamics f.

The safety specification is given as an unsafe region in the state space we want to avoid, denoted as $\mathcal{X}_{\mathcal{U}}$. We consider two notions of a safe set:

1. Avoid Backward Reachable Tube (BRT): The $Avoid$ BRT is the set of initial states from which the system can avoid reaching the unsafe set $\mathcal{X}_{\mathcal{U}}$ over the time horizon t:

$$Avoid(t; \mathcal{X}_{\mathcal{U}}) = \{x \in \mathbb{R}^{n_x} \mid \exists \boldsymbol{u}(\cdot) \text{ s.t. } \forall s \in [-t, 0], \boldsymbol{x}(s) \notin \mathcal{X}_{\mathcal{U}}\}.$$

2. Reach-Avoid BRT: The $ReachAvoid$ BRT is the set of initial states from which the system can reach a target set, specified as $\mathcal{X}_{\mathcal{T}}$, while avoiding the unsafe set $\mathcal{X}_{\mathcal{U}}$:

$$ReachAvoid(t; \mathcal{X}_{\mathcal{T}}, \mathcal{X}_{\mathcal{U}}) = \{x \in \mathbb{R}^{n_x} \mid \exists \boldsymbol{u}(\cdot) \text{ s.t. } \exists s \in [-t, 0], \boldsymbol{x}(s) \in \mathcal{X}_{\mathcal{T}} \;\&\; \forall \tau \in [-t, s], \boldsymbol{x}(\tau) \notin \mathcal{X}_{\mathcal{U}}\}.$$

Here, s corresponds to the time at which the system reaches $\mathcal{X}_{\mathcal{T}}$, and τ indexes over the previous times to ensure that the system does not enter the unsafe set before reaching $\mathcal{X}_{\mathcal{T}}$.

Our goal is to answer two questions: **(i) Safe set construction from data**: how can we estimate these safe sets directly from the trajectory data of the uncertain dynamical system? **(ii) Safe experiment design**: how can we design a sequence of safe experiments that gathers data safely in order to expand the safe set?

B. Hamilton-Jacobi Reachability

HJ reachability encodes the safety problem by first defining a value function whose sign indicates which states are included in the reachable set, and then uses dynamic programming to compute this value function. In this work, we focus on solving the two backward reachability problems described in Section II-A, and other standard reachability problems are detailed in [9]. We first represent the unsafe and target sets as level sets of Lipschitz continuous functions, $g(\cdot)$ and $l(\cdot)$, such that

$$\mathcal{X}_{\mathcal{U}} = \{x \mid g(x) \leq 0\}, \;\; \mathcal{X}_{\mathcal{T}} = \{x \mid l(x) \geq 0\}. \tag{6}$$

Then, we can define the value functions whose zero-superlevel sets represent the $Avoid$ and $ReachAvoid$ BRTs:

Value function for $Avoid$ BRT:

$$V(x,t) := \sup_{\boldsymbol{u}(\cdot)} \min_{s \in [-t,0]} g(\boldsymbol{x}(s)) \tag{7}$$
$$\Rightarrow Avoid(t; \mathcal{X}_{\mathcal{U}}) = \{x \mid V(x,t) \geq 0\}.$$

Value function for $ReachAvoid$ BRT:

$$V(x,t) := \sup_{\boldsymbol{u}(\cdot)} \max_{s \in [-t,0]} \min \left\{ l(\boldsymbol{x}(s)), \min_{\tau \in [-t,s]} g(\boldsymbol{x}(\tau)) \right\} \tag{8}$$
$$\Rightarrow ReachAvoid(t; \mathcal{X}_{\mathcal{T}}, \mathcal{X}_{\mathcal{U}}) = \{x \mid V(x,t) \geq 0\}.$$

The optimization problem in (7) seeks a control that maximizes the closest distance to the unsafe set boundary, and in (8), a control that minimizes the distance to the target set while avoiding $\mathcal{X}_{\mathcal{U}}$.

By applying the dynamic programming principle, the value functions become the viscosity solutions [10] to the following HJ partial differential equations (PDEs) that are in the variational inequality (VI) form [11]:

HJ-VI for $Avoid$ BRT:

$$0 = \min \{g(x) - V(x,t), \; -D_t V(x,t) + H(x, D_x V(x,t))\}, \tag{9}$$
with terminal condition $V(x,0) = g(x)$.

HJ-VI for $ReachAvoid$ BRT:

$$0 = \min \Big\{ g(x) - V(x,t), \tag{10}$$
$$\max\{l(x) - V(x,t), -D_t V(x,t) + H(x, D_x V(x,t))\} \Big\},$$
with terminal condition $V(x,0) = \min\{l(x), g(x)\}$.

In (9) and (10), the *Hamiltonian* $H(x,p)$ is defined as

$$H(x,p) = \max_{u \in U} p^\top f(x,u). \tag{11}$$

To solve (11) directly, we require knowledge of the dynamics f. Even when f is known, (11) may be a nonconvex optimization problem, without further restrictive assumptions such as the control-affineness of f and the convexity of U.

Remark 1. The BRTs guarantee the safety constraint $\boldsymbol{x}(s) \notin \mathcal{X}_{\mathcal{U}}$ only for a finite horizon. Two measures can be taken to guarantee safety for an indefinite horizon. First, we can compute the $Avoid$ BRT for a sufficiently long horizon until the BRT converges to the maximal control invariant set in $\mathcal{X}_{\mathcal{U}}^c$. However, to avoid the issue of discontinuity or non-uniqueness of the HJ-VI solution, a discount factor must be introduced to the value function [12], [13], [14]. An alternative approach is to design the target set in the $ReachAvoid$ BRT as a control invariant set, which results in the finite-time $ReachAvoid$ BRT also being control invariant. We employ the second approach in Section IV for the iterative safe set expansion algorithm.

III. Data-driven Hamiltonian

Our goal is to find a data-driven estimate of the true reachable sets while providing rigorous guarantees on the states included within these sets. Towards this end, we first present the concept of the *data-driven Hamiltonian (DDH)*, which is a lower bound of the Hamiltonian in (11) constructed using the collected trajectory data. We then prove that computing the value function based on DDH yields a conservative estimate (inner-approximation) of the BRTs.

A. Concept

The general idea in our approach is to represent the explicit dynamics abstractly as a state velocity vector $v := f(x,u)$, and adopt a geometric viewpoint of the reachability problem. We define the *vector field bound* (VFB) as the set of possible velocities at a given state $x \in \mathbb{R}^{n_x}$:

$$F(x) = \{f(x,u) \mid u \in U\}. \tag{12}$$

Under this abstraction, the dynamics in (1) can be equivalently represented as the differential inclusion [15],

$$\dot{\boldsymbol{x}}(s) \in F(\boldsymbol{x}(s)), \tag{13}$$

and the Hamiltonian in (11) can be written as

$$H(x,p) := \max_{v \in F(x)} p^\top v, \tag{14}$$

where the objective function in (14) becomes a linear objective in v. We denote $v^* := \arg\max_{v \in F(x)} p^\top v$.

Next, given a single observation in our dataset $\mathcal{D}$, (x^i, u^i, v^i), we reason about what information we have at the state x. Let the *true velocity* at the state x resulting from the observed control $u^i \in U$ be

$$\widetilde{v}^i := f(x,u^i) \quad \in F(x).$$

Since we have observed $v^i = f(x^i,u^i)$, we can construct an uncertain estimate of $\widetilde{v}^i$ around v^i by considering the notion of an *uncertainty set* $\mathcal{E}(x;x^i)$. This set bounds how much the velocity could have changed between x^i and x to satisfy the following requirement:

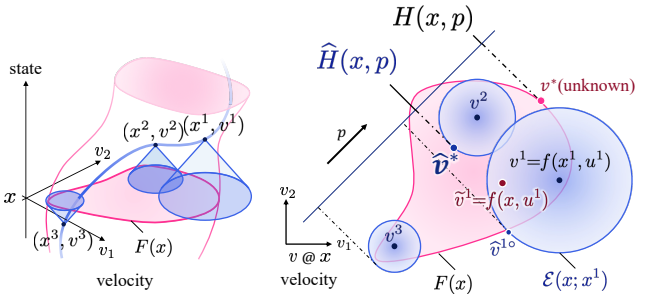

Fig. 1: Illustration of Data-driven Hamiltonian. (left) Velocity space indexed by state. The trajectory data consist of state velocities v^i indexed by states x^i (blue). The true VFB at a query state x, $F(x)$, is unknown (red). We can estimate $F(x)$ by mapping data v^i at x^i to true velocity $\widetilde{v}^i$ at x. (right) Velocity space at x (top-down view of the left). $\widetilde{v}^i$ lies in an uncertainty set $\mathcal{E}(x;x^i)$ propagated from x^i to x (blue circle). Given the costate p, the DDH $\widehat{H}(x,p)$ in (16) takes the best guess $\widehat{v}^*$ among $\widehat{v}^{i\circ}$'s, the worst-case realization of $\widetilde{v}^i \in \mathcal{E}(x;x^i)$. This procedure ensures $\widehat{H}(x,p) \le H(x,p)$.

Assumption 1 (Valid Uncertainty Sets)**.** The uncertainty set, represented as a set-valued map $\mathcal{E} : \mathbb{R}^{n_x} \times \mathbb{R}^{n_x} \to 2^{\mathbb{R}^{n_x}}$, whose output is a closed set in the velocity space, satisfies

$$\widetilde{v}^i - v^i \in \mathcal{E}(x;x^i) \tag{15}$$

or equivalently, $\widetilde{v}^i \in v^i \oplus \mathcal{E}(x;x^i)$, for all $(x^i,u^i,v^i) \in \mathcal{D}$ and $x \in \mathbb{R}^{n_x}$.

Under this assumption, we construct a lower bound on the Hamiltonian by evaluating the minimum of the linear objective $p^\top v$ over the uncertainty set around each observation. This yields our proposed *DDH*:

Data-driven Hamiltonian (DDH):

$$\widehat{H}(x,p) := \max_{i \in \{1,\cdots,N\}} \min_{\widehat{v}^i \in v^i \oplus \mathcal{E}(x;x^i)} p^\top \widehat{v}^i \tag{16}$$

The min operation considers the worst-case realization of the uncertainty associated with each data point and the max operation reasons about what data point provides the best estimate of the Hamiltonian despite the uncertainty.

Notice that for all $i \in \{1,\cdots,N\}$, since $\widetilde{v}^i \in v^i \oplus \mathcal{E}(x;x^i)$ and also $\widetilde{v}^i \in F(x)$,

$$\min_{\widehat{v}^i \in v^i \oplus \mathcal{E}(x;x^i)} p^\top \widehat{v}^i \le p^\top \widetilde{v}^i \le \max_{v \in F(x)} p^\top v = H(x,p).$$

This yields the following proposition:

Proposition 1. If $\mathcal{E}$ satisfies Assumption 1, the DDH is a guaranteed lower bound of the true Hamiltonian:

$$\widehat{H}(x,p) \le H(x,p). \tag{17}$$

Fig. 1 provides a visual explanation of this lower bound mechanism.

B. Practical Implementation

In this section, we describe several instantiations of the uncertainty set and the resulting DDHs by using various levels of system knowledge described in Section II-A. In each case, the DDH is computed by $i^* = \arg\max_{i=\{1,\dots,N\}} p^\top \widehat{v}^{i\circ}$ where $\widehat{v}^{i\circ} = \arg\min_{\widehat{v}^i \in v^i \oplus \mathcal{E}(x;x^i)} p^\top \widehat{v}^i$.

1) l_2-ball DDH: Here we consider the uncertainty sets we can obtain from knowing the uniform Lipschitz constant L^x or the input-element-wise Lipschitz constant vector L^{in}. With L^x, we can use $\mathcal{E}_{L^x}(x;x^i) := \text{B}(L^x \left\|x - x^i\right\|)$, and with L^{in}, we can use $\mathcal{E}_{L^{\text{in}}}(x;x^i) := \text{B}(L^{\text{in}\top}|x - x^i|)$, which guarantees Assumption 1 based on (2) and (3), respectively. Since minimizing a linear objective over an l_2-ball has a closed-form solution, the l_2-ball DDH can be found with

$$\widehat{v}^{i\circ} = v^i - r^i(x)\frac{p}{\|p\|}, \tag{18}$$

where $r^i(x)$ corresponds to the radius of $\mathcal{E}_{L^x}(x;x^i)$ or $\mathcal{E}_{L^{\text{in}}}(x;x^i)$ respectively.

2) Hyperrectangle DDH: Here we consider the uncertainty sets we can obtain from knowing the output-element-wise Lipschitz constant vector L^{out} or the sensitivity matrix L^{io}. With L^{out}, we can use $\mathcal{E}_{L^{\text{out}}}(x;x^i) := \text{Rect}(L^{\text{out}} \left\|x - x^i\right\|)$, and with L^{io}, we can use $\mathcal{E}_{L^{\text{io}}}(x;x^i) := \text{Rect}(L^{\text{io}}|x - x^i|)$. Since minimizing a linear objective over a hyperrectangle has a closed-form solution, both element-wise DDHs can be found with

$$\widehat{v}^{i\circ}_j = \begin{cases} v^i_j - r^i_j(x) & \text{if } p_j \geq 0, \\ v^i_j + r^i_j(x) & \text{otherwise,} \end{cases} \tag{19}$$

where $r^i(x)$ corresponds to the radii of $\mathcal{E}_{L^{\text{out}}}(x;x^i)$ and $\mathcal{E}_{L^{\text{io}}}(x;x^i)$ respectively.

Remark 2. (Computational cost) Fast computation of the DDH is essential since it must be conducted at all state-time grid points for the HJ reachability computation. The DDH computation scales linearly with the number of data points, as it involves solving the inner optimization problem independently for each data point and taking the maximum. The cost of the inner optimization for both the l_2-ball and hyperrectangle DDH scales linearly with the state dimension, as computing the uncertainty set and evaluating the optimization problem are both linear in the state dimension. Therefore, the DDH at a given state x can be computed in $O(Nn_x)$ operations.

C. Additional System Knowledge

We propose additional modifications to the DDH in (16) for when we have further information about the system in order to reduce the gap between $\widehat{H}$ and the true H. For example, physical systems are subject to a reasonable range of state velocities, and we can use this velocity bound to refine our DDH. Suppose we know that a set-valued map $G(x)$ bounds the VFB, satisfying $F(x) \subseteq G(x)$, for all states x within the computation domain. Then,

$$\min_{v\in G(x)} p^\top v \leq \min_{v\in F(x)} p^\top v \leq \max_{v\in F(x)} p^\top v = H(x,p).$$

As a result, we can improve the DDH to $\widehat{H}_G(x,p)$ where

$$\widehat{H}(x,p) \leq \widehat{H}_G(x,p) := \max\left\{\min_{v\in G(x)} p^\top v, \widehat{H}(x,p)\right\} \leq H(x,p).$$

If $G(x)$ consists of simple shapes like hyperspheres or hyperrectangles, $\min_{v\in G(x)} p^\top v$ is computationally inexpensive to evaluate. Using $\widehat{H}_G$ can be an efficient way to reduce the approximation error of our approach in regions where data is scarce and as a result $\mathcal{E}$ is large.

Finally, the DDH can be applied modularly if only a partial component of the system dynamics is uncertain. For instance, if the dynamics consists of two subsystems,

$$\begin{bmatrix}\dot{\boldsymbol{x}}_1(s)\\ \dot{\boldsymbol{x}}_2(s)\end{bmatrix} = \begin{bmatrix}f_1(\boldsymbol{x}_1(s), \boldsymbol{x}_2(s), u_1(s))\\ f_2(\boldsymbol{x}_1(s), \boldsymbol{x}_2(s), u_2(s))\end{bmatrix},$$

where f_1 is unknown and f_2 is known, the Hamiltonian can be decomposed into $H(x,p) = \max_{u_1} p_1^\top f_1(x_1, x_2, u_1) + \max_{u_2} p_2^\top f_2(x_1, x_2, u_2)$. We can replace only the first term with the DDH and keep the second term, which can be computed based on the known model of f_2.

D. Data-driven Value Functions & Safe Sets

Define the *data-driven value functions*, $\widehat{V}(x,t)$, as the solution of the HJ-VIs in (9) and (10), where H is replaced with the DDH $\widehat{H}$ in (16). For instance, $\widehat{V}$ for the $Avoid$ BRT is defined as the solution to

DDH-based HJ-VI for $Avoid$ BRT:

$$0 = \min\left\{g(x) - \widehat{V}(x,t),\ -D_t\widehat{V}(x,t) + \widehat{H}(x, D_x\widehat{V}(x,t))\right\}, \tag{20}$$

with terminal condition $\widehat{V}(x,0) = g(x)$.

We can similarly define the data-driven value function for the $ReachAvoid$ BRT. Presented next is the main theoretical result of this paper.

Theorem 1. The data-driven value function $\widehat{V}(x,t)$ is a *guaranteed lower bound* of the true value function of the BRT problems in (7) and (8):

$$\widehat{V}(x,t) \leq V(x,t). \tag{21}$$

Proof. The main idea of the proof is to reveal the *inverse optimality of the DDH*. We define a fictitious dynamics that captures a differential game between the leader that selects its action among the observed velocities in $\mathcal{D}$, and an adversarial follower that selects its action as the worst-case realization of the uncertain dynamics. Then, we prove that the value function of this game is the viscosity solution of the DDH-HJ-VI (20), $\widehat{V}$. Finally, we show that the true dynamics is always the outcome of a less adversarial follower strategy. See Appendix for the full proof. □

Theorem 2. We define the safe set $S(t) := \{x \mid V(x,t) \geq 0\}$ and the data-driven safe set $\widehat{S}(t) := \{x \mid \widehat{V}(x,t) \geq 0\}$. The safe set $S(t)$ can be either $Avoid(t;\mathcal{X}_\mathcal{U})$ or $ReachAvoid(t;\mathcal{X}_\mathcal{T},\mathcal{X}_\mathcal{U})$. Then, $\widehat{S}(t)$ is a guaranteed inner-approximation of $S(t)$:

$$\widehat{S}(t) \subseteq S(t). \tag{22}$$

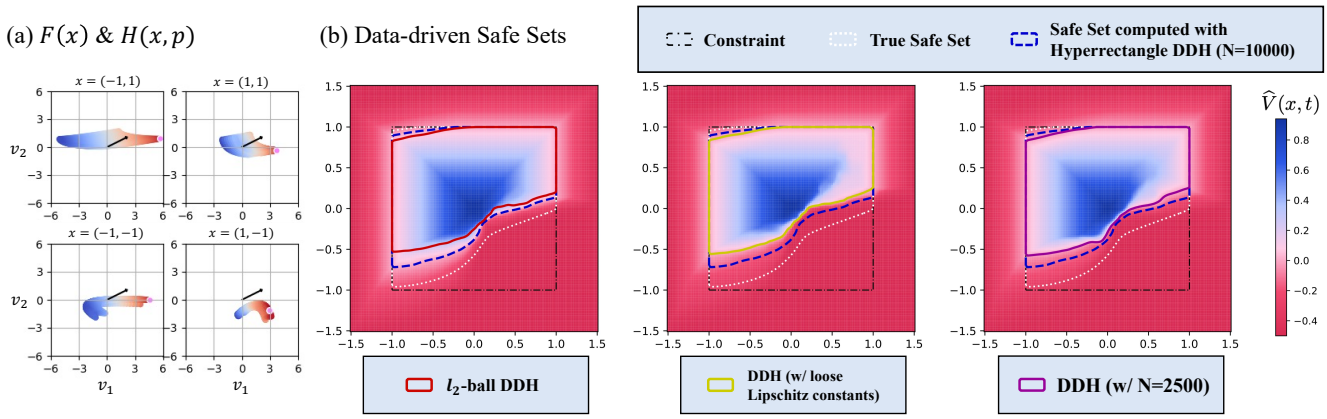

Fig. 2: Random Polynomial Systems. (a) Example of the vector field bound $F(x)$ at various states and $\arg\max_{v\in F(x)} p^\top v$, illustrating the nonconvexity of the optimization. (b) Data-driven safe sets (*Avoid* BRT) computed using the DDH: (1) hyperrectangle DDH using tight sensitivity matrix L^{io} (blue), (2) l_2-ball DDH based on Lipschitz constant L^x (red), (3) hyperrectangle DDH with doubled matrix L^{io} (yellow), and (4) hyperrectangle DDH with fewer data points (purple).

Proof. This is a direct result from (21). □

Finally, the data-driven value function can also provide a safe control policy within the computed safe set $\widehat{S}(t)$. Define

$$\pi_{\widehat{V}}(x,-t) = u^{i*}, \tag{23}$$

where

$$i^* = \underset{i\in\{1,\cdots,N\}}{\arg\max} \min_{\widehat{v}^i \in v^i \oplus \mathcal{E}(x;x^i)} D_x\widehat{V}(x,t)^\top \widehat{v}^i$$

is the solution of the optimization in (16). When we try to maximize $\widehat{V}$, if we take u^{i*} as our control, we are guaranteed to do better than the worst-case instantiation of the uncertainty. That is,

$$\widehat{H}(x, D_x\widehat{V}(x,t)) \le D_x\widehat{V}(x,t)^\top f(x,u^{i*}).$$

This means that $\pi_{\widehat{V}}(\boldsymbol{x}(s),s)$ can maintain safety, $\boldsymbol{x}(s) \notin \mathcal{X}_{\mathcal{U}}$ for $s \in [-t,0]$. For the reach-avoid problem, we are guaranteed to reach the target set no later than t under $\pi_{\widehat{V}}$ for any initial state in $ReachAvoid(t;\mathcal{X}_{\mathcal{T}},\mathcal{X}_{\mathcal{U}})$.

E. Running Example: Random Polynomial Systems

We consider a system with $n_x = n_u = 2$ with dynamics $f_i(x) = p_i(u_1,u_2)+q_i(u_1,u_2)x_1+r_i(u_1,u_2)x_2$, for $i=1,2$, where p_i, q_i, r_i are quadratic polynomials in u with randomly generated coefficients in $[-2,2]$. The constant terms of p_i are set to zero so that $x=0$ is an equilibrium under $u=0$. The randomness in the coefficients yields various nonconvex shapes for the VFB $F(x)$ at each state. Using the first-order optimality condition, we analytically solve for the true Hamiltonian (Fig. 2 (a)), from which we compute a true safe set to validate our DDH-based safe sets. Tight Lipschitz constants can also be computed analytically from the coefficients. In applying our methods, we assume no explicit knowledge of the dynamics, treating them as a black-box model. The dataset $\mathcal{D}$ is obtained by uniform sampling across the state domain and control bounds. In practice, collecting such data safely is challenging; we address realistic safe data collection further in the next section.

Fig. 2 (b) shows safe sets computed using the *Avoid* BRT formulation with four DDH instantiations. In all cases, the resulting sets correctly under-approximate the true safe set. Tighter Lipschitz bounds and larger datasets generally produce less conservative safe sets. However, not only the amount but also the informational content of the data significantly influences the safe set construction. Careful balancing between required prior information (e.g., Lipschitz bounds), data quantity and quality, and the resulting conservatism remains an important direction for future investigation.

IV. Iterative Safe Set Expansion

In this section, we introduce an algorithm for iteratively updating a data-driven *ReachAvoid* BRT while maintaining safety throughout the data collection process. Our algorithm is motivated by the test procedure of real-world systems for safety verification—such as flight envelope expansion, which will be illustrated in Section V—where experiments start from an initial conservative safe region, designed with, for instance, local linear analysis. As such, we make the following assumption:

Assumption 2. The target set $\mathcal{X}_{\mathcal{T}}$ must be *forward invariant* under a *backup policy* $\pi^{\text{backup}}(x)$ and must not intersect with the unsafe set, $\mathcal{X}_{\mathcal{T}} \cap \mathcal{X}_{\mathcal{U}} = \emptyset$.

The target set is by definition contained in the safe set (the *ReachAvoid* BRT) even when no data is collected. Thus, we can safely initiate the data collection by setting the initial estimate of the safe set $\widehat{S}_0$ as $\mathcal{X}_{\mathcal{T}}$ and using π^{backup} for the initial experiments.

Overview (Algorithm 1). At each iteration k, we start the procedure by sampling initial conditions $\{x_0^j\}_{j=1}^{n_{\text{traj}}}$ from the current data-driven safe set $\widehat{S}_k$. We then roll out trajectories from each initial condition using a policy that is guaranteed to maintain the trajectory within $\widehat{S}_k$, denoted by π_k. The data from these rollouts are appended to the current dataset, yielding a new dataset $\mathcal{D}_{k+1}$ which is then used to compute the next iteration's data-driven safe set $\widehat{S}_{k+1}$. A data reduction step is applied at the end of each iteration to reduce

Algorithm 1: Safe experiments for safe set expansion

Input: $\mathcal{X}_\mathcal{T} = \{l(x) \geq 0\}$: Control invariant target set,
$\mathcal{X}_\mathcal{U} = \{g(x) \leq 0\}$: Unsafe set,
π^{backup}: Backup policy, π^{exp}: Exploration policy,
n^{iter}: Number of iterations,
n^{traj}: Number of experiments per iteration,
T: Time length of each rollout, Δt: sampling time,
$\mathsf{GetInit}(S; n^{\text{traj}}, \mathcal{D}, V)$: Selects initial states within the safe set S, given the dataset $\mathcal{D}$ and value function V,
$\mathsf{Rollout}(\pi; x_0)$: Obtains trajectory under policy π by running experiment with initial state x_0,
$\mathsf{PruneData}(\mathcal{D}, V)$: Conducts data reduction based on the value function V.
Output: Final safe set $\widehat{S}_{n^{\text{iter}}}$

Initialization: $\mathcal{D}_0 = \{\}$, $\widehat{S}_0 \leftarrow \mathcal{X}_\mathcal{T}$, $\pi_0^{\text{safe}} \leftarrow \pi^{\text{backup}}$
for $k \leftarrow 0$ **to** n^{iter} **do**
  $\{x_0^j\}_{j=1}^{n^{\text{traj}}} \leftarrow \mathsf{GetInit}(\widehat{S}_k; n^{\text{traj}}, \mathcal{D}_k, \widehat{V}_k)$
  $\mathcal{D}_{k+1} \leftarrow \mathcal{D}_k$
  for $j \leftarrow 1$ **to** n^{traj} **do**
    $\pi_k(x) \leftarrow$ (24) based on $\pi^{\text{backup}}, \pi_k^{\text{safe}}, \pi^{\text{exp}}$.
    $\{x^i, u^i, v^i\}_{i=0}^{\lfloor \mathrm{T}/\Delta t \rfloor} \leftarrow \mathsf{Rollout}(\pi_k; x_0^j)$
    $\mathcal{D}_{k+1} \leftarrow \mathcal{D}_{k+1} \cup \{x^i, u^i, v^i\}_{i=0}^{\lfloor \mathrm{T}/\Delta t \rfloor}$
  end
  $\widehat{V}_{k+1} \leftarrow$ Compute (20) with $\mathcal{D}_{k+1}$
  $\widehat{S}_{k+1}, \pi_{k+1}^{\text{safe}} \leftarrow$ Update from $\widehat{V}_{k+1}, \mathcal{D}_{k+1}$
  $\mathcal{D}_{k+1} \leftarrow \mathsf{PruneData}(\mathcal{D}_{k+1}, \widehat{V}_{k+1})$
end

the computational expense of the process and retain only the data most relevant to safety.

Initial States. The initial states are sampled near the boundary of the data-driven safe set $\widehat{S}_k$. Sampling initial states close to the boundary reduces the conservatism of the DDH at the boundary, thus helping to expand the safe set. The existing data in $\mathcal{D}$ can also guide the selection of the initial states, for example by encouraging the selection of states in regions with less data.

Safe Exploration Policy. The safe exploration policy π_k is defined as

$$\pi_k(x) = \begin{cases} \pi^{\text{backup}}(x) & \text{if } l(x) \geq 0, \\ \pi_k^{\text{safe}}(x) & \text{if } l(x) < 0 \;\&\; \widehat{V}_k(x,t) < \epsilon, \\ \pi^{\text{exp}}(x) & \text{otherwise,} \end{cases} \quad (24)$$

with safety threshold $\epsilon > 0$, where t is the time horizon of the *ReachAvoid* BRT. If the system is in the target set, we apply the backup controller, which is guaranteed to keep it within the set by Assumption 2. If the state is outside the target set and away from the safe set boundary ($\widehat{V}_k(x,t) \geq \epsilon$), we apply an exploration policy π^{exp} which does not need to satisfy any particular safety constraint. Finally, when the state is close to exiting the safe set ($\widehat{V}_k(x,t) < \epsilon$), we apply the safety controller of the current data-driven safe set, $\pi_k^{\text{safe}}(x) = \pi_{\widehat{V}_k}(x, -t)$, where $\pi_{\widehat{V}_k}$ is defined in (23). Regardless of the exploration policy π^{exp}, the system under this switching safety filter can stay within $\widehat{S}_k$ due to its control invariance noted in Remark 1 [16].

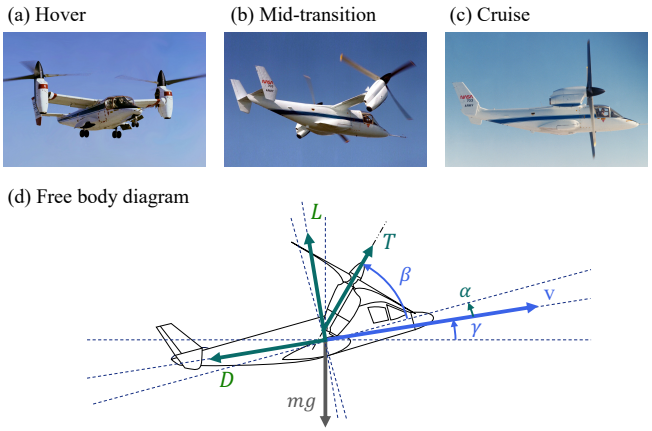

Fig. 3: (a)-(c) NASA-Army-Bell XV-15 tiltrotor aircraft in various rotor configurations (Source: NASA). (d) Free body diagram of XV-15 for its longitudinal dynamics in (25).

Proposition 2. If $\widehat{S}_0 = \mathcal{X}_\mathcal{T}$ and π^{backup} satisfy Assumption 2, the trajectories in Algorithm 1 never enter $\mathcal{X}_\mathcal{U}$.

Proof. Consider an arbitrary iteration k, with current data-driven safe set $\widehat{S}_k$ from dataset $\mathcal{D}_k$. The initial state is contained in $\widehat{S}_k$. As a result, since π_k renders $\widehat{S}_k$ forward invariant, the resulting trajectory will be contained in $\widehat{S}_k$. Since $\widehat{S}_k$ is a *ReachAvoid* BRT, $\widehat{S}_k \cap \mathcal{X}_\mathcal{U} = \emptyset$. □

Data Reduction. We apply a data reduction that removes data points irrelevant to safety. This consists of keeping only the data whose indices show up as the optimal i^* for the DDH evaluated during the computation of the value function $\widehat{V}_k$. These data points are the ones actually used in the computation of $\widehat{V}_k$ and the resulting data-driven safe control. This reduction significantly helps the computation time with negligible impact on the resulting safe set.

Design Decisions. A variety of design choices influence the outcome of the algorithm. In particular, the sampling strategy for initial states and the exploration policy π^{exp} have been empirically shown to be decisive factors in the efficiency of the safe set expansion. Additional parameters, including n^{traj} and the experiment length T, also affect the result. A more in-depth investigation into the varying effects of these design choices is left for future work.

V. Application to Tiltrotor Safety Verification

Recent progress in electric propulsion technologies has enabled various novel vertical take-off and landing (VTOL) aircraft designs to emerge. However, verifying the flight envelope of these vehicles is challenging due to their flight mode transitions between hover and cruise. During these transitions, the vehicle faces a precarious balance between rotor propulsion and aerodynamic lift, alongside highly uncertain aerodynamic interactions between the rotors and the airframe, significantly increasing the risk of loss of control [17]. This vulnerability becomes particularly apparent during flight tests in product development, where experiments to

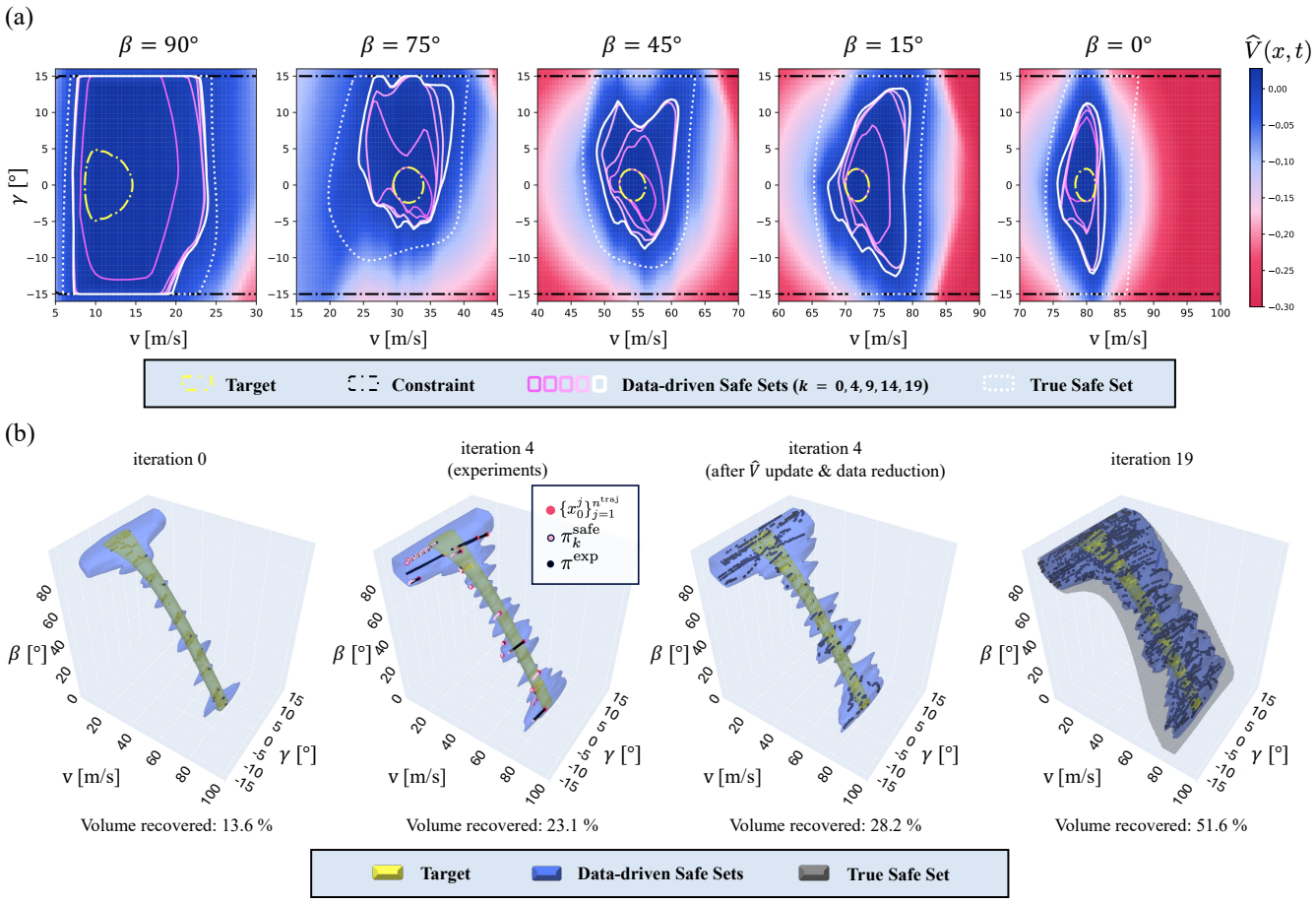

Fig. 4: XV-15 safe set expansion conducted for 20 iterations under Algorithm 1, during its flight mode transition from near-hover ($\beta = 90°$) to cruise ($\beta = 0°$). (a) Data-driven safe sets at various iterations, shown as 2D slices in v-γ at various tilt angles β. (b) The safe sets shown in 3D state space at iterations $k = 0, 4, 19$. At each iteration, the trajectories are collected under the data-driven safety-filtered exploration policy, ensuring that they stay within the previous iteration's safe set. After the safe set is updated based on new data, data reduction is conducted to prune data irrelevant for safe set computation.

expand the vehicle's flight envelope must be conducted without an accurate model available a priori. This motivates applying our framework in Section IV to VTOL vehicle flight envelope verification while treating the underlying dynamics as uncertain. Previously, HJ reachability was adopted in [18], [19], [20] to verify the flight envelope of aircraft using explicit dynamics models.

We consider the XV-15 [21], a tiltrotor vehicle (Fig. 3), transitioning from vertical to forward flight. Its mathematical model in [22] is used for simulation and validating our results. We construct the *ReachAvoid* BRT from which safe recovery to a near-hover trim condition is guaranteed. Our algorithm gradually expands the BRT while ensuring safety during experiments for new data collection, analogous to the procedure of flight envelope expansion in flight tests.

Implementation Details. We consider the reduced-order longitudinal dynamics of the vehicle detailed in [22], [23]. The state consists of $x = [\mathrm{v}, \gamma, \beta]^\top$, where v is the airspeed, γ is the flight path angle, and β is the rotor tilt angle ($\beta = 0°$ in cruise configuration), and the control input is $u = [T, \alpha, \delta]$, where T is the rotor thrust, α is the angle of attack, and δ is the rotor tilt angle rate. The equation of motion is given as

$$\begin{bmatrix} \dot{\mathrm{v}} \\ \dot{\gamma} \end{bmatrix} = -g \begin{bmatrix} \sin\gamma \\ \frac{\cos\gamma}{\mathrm{v}} \end{bmatrix} + \frac{1}{m} \left(\begin{bmatrix} \cos(\alpha+\beta) \\ \frac{\sin(\alpha+\beta)}{\mathrm{v}} \end{bmatrix} T + \begin{bmatrix} -D(\mathrm{v},\alpha,\beta) \\ \frac{L(\mathrm{v},\alpha,\beta)}{\mathrm{v}} \end{bmatrix} \right), \quad (25)$$

where L and D are the lift and drag forces that vary with respect to $\mathrm{v}, \alpha, \beta$, which constitutes the main nonlinearity and uncertainty source in the dynamics. For the true safe set computation, since the true Hamiltonian involves a nonconvex optimization, we approximately solve it by evaluating it over a set of discretized control inputs and then taking the maximum. For the DDH, we treat $\dot{\beta} = \delta$ as a known portion of the dynamics and apply the technique in Section III-C. We use the hyperrectangle DDH based on a sensitivity matrix whose values are estimated from the flight data in [22].

We consider $\gamma \in [-15°, 15°]$ as our primary safety constraint, restraining the vehicle from extreme vertical speed, and an additional lower-bound on airspeed at each tilt angle varying from 5m/s (near-hover) to 50m/s (cruise). The initial safe set (i.e. the target set) is designed based on the LQR funnel around the transition trim corridor of the vehicle, detailed in [23]. If the vehicle can reach this trim corridor, it can successfully recover to the near-hover trim state. The

associated LQR control at each trim point on the corridor serves as the backup controller π^{backup} that maintains the target set forward invariant. For the exploration policy π^{exp}, we apply a control input with Gaussian noise centered around a mean value randomly selected for each experiment. The mean bias term incentivizes trajectories to explore various directions. We use $n^{\text{traj}} = 50$ for $k = 0$, and $n^{\text{traj}} = 20$ for subsequent iterations, with each trajectory length $\mathrm{T} = 1\mathrm{s}$ and sampling time $\Delta t = 0.01\mathrm{s}$.

The DDH solution and the numerical solver of the DDH-based HJ-VI are implemented in PyTorch, based on the level set method in [24]. Using GPU for parallel computation, each iteration takes around 40 minutes on Nvidia RTX 4090, for the state grid with size $(191 \times 50 \times 101)$, time horizon $t = 1\mathrm{s}$, and the number of data points N around 5,000.

Results. The data-driven safe sets resulting from conducting the experiments under Algorithm 1 are visualized in Fig. 4. After 20 iterations, we recover 51.6% of the volume of the true safe set within the verified data-driven safe set, and each data-driven safe set is a successful inner-approximation. We also observe that the safe exploration policy designed in (24) guarantees the safety of all experiments. Finally, by applying the data reduction technique, we reduced 43,000 data points sampled from trajectories to 4,294 points in the final result.

VI. Conclusion & Future Work

We propose a direct data-driven framework for constructing safe sets from trajectory data. This framework produces safe sets that are guaranteed to be subsets of the true safe set while only requiring knowledge of a Lipschitz constant of the dynamics. We also present an approach to iteratively expand these safe sets while maintaining safety. The core of this framework and our main contribution is the data-driven Hamiltonian (DDH), a data-driven lower bound of the Hamiltonian used in Hamilton-Jacobi (HJ) reachability analysis. Without needing an explicit dynamics model, the DDH provides a new paradigm for how model-based analysis and prior knowledge can be integrated with data-driven approaches in order to ensure safety.

Our proposed approach has several limitations. The numerical methods used in this work for the reachability computation suffer from the curse of dimensionality, and our DDH scales linearly with the number of data points, which can lead to the problem being intractable in higher dimensions or on large datasets. While we mitigate this through parallelization on GPUs and data reduction, further studies are required to improve the scalability of the computation. The DDH also relies on knowledge of a Lipschitz constant, whose tight value may be challenging to estimate in advance. Finally, our switching filter is rudimentary and may have issues in practice like chattering. In future work, we plan to investigate the effects of the design choices in the iterative safe set expansion algorithm, explore the use of more advanced safety filters, and extend the DDH to other control problems.

Acknowledgements

We thank Shaun Mcwherter and Thomas Lombaerts at NASA for the insightful discussions.

Appendix: Proof of Theorem 1

For conciseness, we only conduct the proof for the $Avoid$ BRT value functions. Proof for the $ReachAvoid$ value function can be done similarly. We consider three dynamical systems and their corresponding BRT value functions:

1) The original dynamics $\boldsymbol{x}(\cdot)$ in (1) and (13), and its value function $V(x,t)$ in (7).
2) The original dynamics but whose control is confined to the ones in the dataset, $\dot{\widetilde{\boldsymbol{x}}}(s) = f(\widetilde{\boldsymbol{x}}(s), \widetilde{\boldsymbol{u}}(s)), \widetilde{\boldsymbol{x}}(-t) = x$, with $\widetilde{\boldsymbol{u}}(s) \in \mathcal{D}_u := \{u^i\}_{i=1}^N$. The BRT value function is given as $\widetilde{V}(x,t) = \sup_{\widetilde{\boldsymbol{u}}(\cdot)} \min_{s\in[-t,0]} g(\widetilde{\boldsymbol{x}}(s))$.
3) A fictitious dynamics that captures a differential Stackelberg game between the leader $\boldsymbol{v}$ and the follower $\boldsymbol{w}$, whose trajectory is defined as
$$\dot{\widehat{\boldsymbol{x}}}(s) = \boldsymbol{v}(s) + \boldsymbol{w}(s), \quad \widehat{\boldsymbol{x}}(-t) = x. \tag{26}$$
The leader's action is confined by $\boldsymbol{v}(s) \in \mathcal{D}_v := \{v_i\}_{i=1}^N$, and the follower's action is confined based on the current state and the leader's action, $\boldsymbol{w}(s) \in W(\widehat{\boldsymbol{x}}(s), \boldsymbol{v}(s))$. The follower's action set is defined as the uncertainty sets for DDH in (15), i.e., $W(x, v_j) \equiv \mathcal{E}(x; x_j)$, when $\boldsymbol{v}(s) = v_j \in \mathcal{D}_v$. In other words, the leader selects the velocity in the dataset, and the follower selects the uncertainty vector within the uncertainty set associated with each data.

   The BRT value function of this game is defined as
$$\widehat{V}(x,t) := \inf_{\xi_w} \sup_{\boldsymbol{v}(\cdot)} \min_{s\in[-t,0]} g(\widehat{\boldsymbol{x}}(t)), \tag{27}$$
   where ξ_w is the follower's non-anticipative strategy [25], in response to the leader, a mapping from $\boldsymbol{v}(\cdot)$ to $\boldsymbol{w}(\cdot)$.

Theorem 1 is proved by showing that a) $\widehat{V}$ in (27) is the unique viscosity solution of the HJ-VI in (20) (Theorem 3), and b) $\widehat{V}(x,t) \le \widetilde{V}(x,t) \le V(x,t)$ (Theorem 4). □

Theorem 3 (Viscosity solution theorem)**.** $\widehat{V}$ defined in (27) is the unique viscosity solution to the HJ-VI in (20).

Proof. We first see that the Hamiltonian of $\widehat{V}$ in (27) is indeed the DDH:
$$\max_{v\in\mathcal{D}_v} \min_{w\in W(x,v)} p^\top (v+w) = \max_{i\in\{1,\cdots,N\}} \min_{w\in W(x,v_i)} p^\top (v_i + w)$$
$$= \max_{i\in\{1,\cdots,N\}} \min_{\widehat{v}_i \in v_i \oplus \mathcal{E}(x;x_i)} p^\top \widehat{v}_i = \widehat{H}(x,p),$$
where $\widehat{v}_i = v_i + w$. The rest of the proof can be adopted from the viscosity solution theorem for differential games in [25, Thm. 4.1], as similarly done in [26], [11] for the HJ-VIs. The noticeable differences in our assumptions from those of [25, Thm. 4.1] are 1) $\mathcal{D}_v$ is not a compact set in our case, and 2) the follower's action space $W(x,v)$ is conditioned on the leader's action v. This requires the adoption of [25, Lemma 4.3], used for the proof of [25, Thm. 4.1], to our settings as Lemma 1 below. The lemma is the crucial step that translates the inf-sup leader and follower objectives in $\widehat{V}$ to max-min objectives in $\widehat{H}$. The uniqueness follows from [27, Thm. 4.2]. □

Lemma 1. (Adoption of [25, Lemma 4.3]) For $\phi(x,t) \in C^1$, (a) If $\exists \theta > 0$, $\exists (x_0, t_0) \in \mathbb{R}^n \times \mathbb{R}_{<0}$ such that

$$\max_{v \in \mathcal{D}_v} \min_{w \in W(x,v)} D_t\phi(x,t) + D_x\phi(x,t)^\top (v+w) \leq -\theta, \quad (28)$$

then there exists a small enough $\delta > 0$, and the follower's non-anticipative strategy ξ_w such that for all $\boldsymbol{v}(\cdot)$,

$$\phi(\widehat{\boldsymbol{x}}(t_0+\delta), t_0+\delta) - \phi(x_0,t_0) \leq -\frac{\theta}{2}\delta. \quad (29)$$

(b) If $\exists \theta > 0$, $\exists (x_0, t_0) \in \mathbb{R}^n \times \mathbb{R}_{<0}$ such that

$$\max_{v \in \mathcal{D}_v} \min_{w \in W(x,v)} D_t\phi(x,t) + D_x\phi(x,t)^\top (v+w) \geq \theta,$$

there exists a small enough $\delta > 0$, such that for all follower's non-anticipative strategy ξ_w, there exists the leader's control signal $\boldsymbol{v}(\cdot)$ such that $\phi(\widehat{\boldsymbol{x}}(t_0+\delta), t_0+\delta) - \phi(x_0,t_0) \geq \frac{\theta}{2}\delta$.

Proof. Proof of (a): Due to condition (28), for each $v_i \in \mathcal{D}_v$, there exists $w = \widehat{w}(v_i)$ such that

$$D_t\phi(x_0,t_0) + D_x\phi(x_0,t_0)^\top (v_i + \widehat{w}(v_i)) \leq -\theta.$$

Due to the C^1 property of ϕ, we have

$$D_t\phi(\widehat{\boldsymbol{x}}(s),s) + D_x\phi(\widehat{\boldsymbol{x}}(s),s)^\top (v_i + \widehat{w}(v_i)) \leq -\frac{\theta}{2}, \quad (30)$$

for small enough $\delta > 0$, and $s \in [t_0, t_0+\delta]$. Consider the follower's disturbance strategy ξ_w that satisfies $\xi_w[\boldsymbol{v}](s) = \widehat{w}(\boldsymbol{v}(s))$ for $s \in [t_0, t_0+\delta]$. From (30), we have

$$D_t\phi(\widehat{\boldsymbol{x}}(s),s) + D_x\phi(\widehat{\boldsymbol{x}}(s),s)^\top (\boldsymbol{v}(s) + \xi_w[\boldsymbol{v}](s)) \leq -\frac{\theta}{2},$$

$\forall s \in [t_0, t_0+\delta]$. Integration from t_0 to $t_0+\delta$ results in (29). Proof of (b) can be adopted directly from [25]. □

Theorem 4. $\widehat{V}(x,t) \leq \widetilde{V}(x,t) \leq V(x,t)$ $\forall x \in \mathbb{R}^n$, $t \geq 0$.

Proof. The second inequality is trivial by observing that $\mathcal{D}_u \subset U$. We consider a non-anticipative strategy of the follower, $\widetilde{\xi}_w$, selecting its action as:

$$\widetilde{\xi}_w[\boldsymbol{v}(s)] \equiv f(\widehat{\boldsymbol{x}}^{\widetilde{\xi}_w}(s), \widehat{\boldsymbol{u}}(s)) - \boldsymbol{v}(s), \quad (31)$$

where $\widehat{\boldsymbol{u}}(s) = u_j$ for $\boldsymbol{v}(s) = v_j \in \mathcal{D}_v$ at each $s \in [-t, 0]$, and $\widehat{\boldsymbol{x}}^{\widetilde{\xi}_w}(s)$ solves (26) with $\boldsymbol{w}(s) \equiv \widetilde{\xi}_w[\boldsymbol{v}(s)]$. Note that this strategy is non-anticipative since we don't use any information of the follower's action in $\tau \in (s, 0]$. More importantly, it is a *feasible* strategy because for $\boldsymbol{v}(s) = v_j$,

$$f(\widehat{\boldsymbol{x}}^{\widetilde{\xi}_w}(s), u_j) - v_j \in \mathcal{E}(\widehat{\boldsymbol{x}}^{\widetilde{\xi}_w}(s); x_j) = W(\widehat{\boldsymbol{x}}^{\widetilde{\xi}_w}(s), \boldsymbol{v}(s)).$$

Under this follower strategy $\widetilde{\xi}_w$, (26) becomes

$$\dot{\widehat{\boldsymbol{x}}}^{\widetilde{\xi}_w}(s) = \boldsymbol{v}(s) + \widetilde{\xi}_w[\boldsymbol{v}(s)] = f(\widehat{\boldsymbol{x}}^{\widetilde{\xi}_w}(s), \widehat{\boldsymbol{u}}(s)).$$

Intuitively, the follower always selects its action so that the fictitious dynamics (26) become identical to the original dynamics. As a result, we can see that with $\widetilde{\boldsymbol{u}} \equiv \widehat{\boldsymbol{u}}$,

$$\sup_{\boldsymbol{v}(\cdot)} \min_{s \in [-t,0]} g(\widehat{\boldsymbol{x}}^{\widetilde{\xi}_w}(t)) \equiv \widetilde{V}(x,t),$$

Since $\widehat{V}$ minimizes the identical cost function over all possible follower strategies, we get $\widehat{V}(x,t) \leq \widetilde{V}(x,t)$. □

REFERENCES

[1] S. Bansal, M. Chen, S. L. Herbert, and C. J. Tomlin, "Hamilton-Jacobi reachability: A brief overview and recent advances," in *IEEE Conference on Decision and Control (CDC)*, 2017.

[2] J. F. Fisac, A. K. Akametalu, M. N. Zeilinger, S. Kaynama, J. Gillula, and C. J. Tomlin, "A general safety framework for learning-based control in uncertain robotic systems," *IEEE Transactions on Automatic Control (TAC)*, 2019.

[3] V. K. Chilakamarri, Z. Feng, and S. Bansal, "Reachability analysis for black-box dynamical systems," *arXiv preprint arXiv:2410.07796*, 2024.

[4] A. Devonport, F. Yang, L. El Ghaoui, and M. Arcak, "Data-driven reachability analysis with Christoffel functions," in *IEEE Conference on Decision and Control (CDC)*, 2021.

[5] F. Djeumou, A. P. Vinod, E. Goubault, S. Putot, and U. Topcu, "On-the-fly control of unknown smooth systems from limited data," in *2021 American Control Conference (ACC)*, 2021.

[6] A. Alanwar, A. Koch, F. Allgöwer, and K. H. Johansson, "Data-driven reachability analysis from noisy data," *IEEE TAC*, 2023.

[7] T. Lew and M. Pavone, "Sampling-based reachability analysis: A random set theory approach with adversarial sampling," in *Conference on Robot Learning*, 2021.

[8] S. S. Sastry, *Nonlinear systems: analysis, stability, and control*. Springer Science & Business Media, 2013, vol. 10.

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

[10] M. Bardi, I. C. Dolcetta, *et al.*, *Optimal control and viscosity solutions of Hamilton-Jacobi-Bellman equations*. Springer, 1997, vol. 12.

[11] J. F. Fisac, M. Chen, C. J. Tomlin, and S. S. Sastry, "Reach-avoid problems with time-varying dynamics, targets and constraints," in *International Conference on Hybrid Systems: Computation and Control (HSCC)*, 2015.

[12] A. K. Akametalu, S. Ghosh, J. F. Fisac, and C. J. Tomlin, "A minimum discounted reward Hamilton-Jacobi formulation for computing reachable sets," *arXiv preprint arXiv:1809.00706*, 2018.

[13] B. Xue, Q. Wang, N. Zhan, M. Fränzle, and S. Feng, "Differential games based on invariant sets generation," in *2022 American Control Conference (ACC)*, 2022.

[14] J. J. Choi, D. Lee, B. Li, J. P. How, K. Sreenath, S. L. Herbert, and C. J. Tomlin, "A forward reachability perspective on robust control invariance and discount factors in reachability analysis," *arXiv preprint arXiv:2310.17180*, 2023.

[15] R. Goebel, R. G. Sanfelice, and A. R. Teel, "Hybrid dynamical systems," *IEEE Control Systems Magazine (CSM)*, 2009.

[16] K. P. Wabersich, A. J. Taylor, J. J. Choi, K. Sreenath, C. J. Tomlin, A. D. Ames, and M. N. Zeilinger, "Data-driven safety filters: Hamilton-Jacobi reachability, control barrier functions, and predictive methods for uncertain systems," *IEEE CSM*, 2023.

[17] C. M. Belcastro, J. V. Foster, G. H. Shah, I. M. Gregory, D. E. Cox, D. A. Crider, L. Groff, R. L. Newman, and D. H. Klyde, "Aircraft loss of control problem analysis and research toward a holistic solution," *Journal of Guidance, Control, and Dynamics*, 2017.

[18] A. M. Bayen, I. M. Mitchell, M. M. Oishi, and C. J. Tomlin, "Aircraft autolander safety analysis through optimal control-based reach set computation," *Journal of Guidance, Control, and Dynamics*, 2007.

[19] T. Lombaerts, S. Schuet, K. Wheeler, D. M. Acosta, and J. Kaneshige, "Safe maneuvering envelope estimation based on a physical approach," *AIAA Guidance, Navigation, and Control Conference*, 2013.

[20] T.-W. Hsu, J. J. Choi, D. Amin, C. J. Tomlin, S. C. McWherter, and M. Piedmonte, "Towards flight envelope protection for the nasa tiltwing evtol flight mode transition using Hamilton-Jacobi reachability," *Journal of the American Helicopter Society*, 2024.

[21] M. D. Maisel, "The history of the XV-15 tilt rotor research aircraft: from concept to flight," *NASA SP-2000-4517*, 2000.

[22] S. W. Ferguson, "A mathematical model for real time flight simulation of a generic tilt-rotor aircraft," *NASA CR-166536*, 1988.

[23] T. Lombaerts, K. Shish, and J. Kaneshige, "Trim envelope calculations for a tiltrotor in forward flight, hover and transitions," in *11th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes*, 2022.

[24] I. M. Mitchell, *Application of level set methods to control and reachability problems in continuous and hybrid systems*. Stanford University, 2002.

[25] L. C. Evans and P. E. Souganidis, "Differential games and representation formulas for solutions of Hamilton-Jacobi-Isaacs equations," *Indiana University Mathematics Journal*, 1984.

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

[27] E. Barron and H. Ishii, "The bellman equation for minimizing the maximum cost." *Nonlinear Anal. Theory Methods Applic.*, 1989.