Adversarial Physics-Informed Learning for Robust Optimal Safe Control in Time-Critical Environments: A Game-Theoretic Approach

Nick-Marios T. Kokolakis[1], Shanqing Liu[2], Jérôme Darbon[2], Rahul Mangharam[1], and George Em. Karniadakis[2]

Abstract— **Autonomous systems operating in adversarial and time-critical environments require strategic decision-making mechanisms that ensure safety, robustness, and performance. Safe predefined-time stability characterizes parameter-dependent nonlinear dynamical systems whose trajectories starting in a set of admissible states remain within the set and converge to an equilibrium point within a predefined time. In this paper, we develop a game-theoretic framework to address a robust optimal safe predefined-time stabilization problem for parameter-dependent nonlinear dynamical systems subject to an adversary with nonquadratic performance measures. In particular, the robust optimal safe predefined-time stabilization problem is formulated as a two-player zero-sum differential game, wherein the controller is a minimizing player and the adversary is a maximizing player. Sufficient conditions for the existence of a saddle-point solution to the zero-sum game and closed-loop system safe predefined-time stability are derived. Specifically, safe predefined-time stability of the closed-loop system is guaranteed via a barrier Lyapunov function satisfying a differential inequality while serving as a solution to the steady-state Hamilton–Jacobi–Isaacs (HJI) equation ensuring Nash equilibrium. Since the steady-state HJI equation is typically intractable to solve analytically, we construct an adversarially robust physics-informed machine learning algorithm to learn the safely predefined-time stabilizing solution to the steady-state HJI equation. Simulation results illustrate the efficacy of the proposed framework.**

I. Introduction

Autonomy pertains to controlled systems that can operate without human intervention. Systems with this capability are termed autonomous systems (ASs), such as self-driving cars, humanoid robots, and unmanned aerial vehicles [1]. However, numerous incidents of unintended AS crashes highlight that ASs are *safety-critical systems*. Hence, ensuring safety has led to the emergence of *safe autonomy* [2]. Safe autonomy can be enabled by harnessing the advantages of *nonlinear control theory* [3], *optimal control theory* [4], *robust control theory* [5], and *game theory* [6] to equip ASs with control architectures that ensure safety, stability, robustness, and performance. However, ensuring safety becomes considerably more challenging in the presence of adversarial disturbances arising from cyber-physical attacks. This necessitates the synthesis of adversarially robust optimal safe policies guaranteeing disturbance rejection in a predefined time. Incorporating *predefined-time adversarial robustness* into safe control design enhances resilience and reliability in real-world applications.

Stability theory concerns the behavior of the system trajectories of a dynamical system when the system initial state is near an equilibrium state [3]. The notion of *asymptotic stability* allows the convergence of system trajectories to a Lyapunov stable equilibrium point over an infinite horizon [3]. In contrast, the concept of *finite-time stability* enables the convergence of system solutions to a Lyapunov stable equilibrium state in finite time [7]. However, the settling-time function for finite-time stability is not uniformly bounded, and hence the convergence time may increase (possibly unboundedly) with the norm of the initial condition. *Fixed-time stability* strengthens the notion of finite-time stability by guaranteeing that the settling-time function is uniformly bounded with respect to the initial condition [8]. However, this upper bound cannot be prescribed a priori. Alternatively, the concept of *predefined-time stability* involves fixed-time stable parameter-dependent dynamical systems whose upper bound of the settling-time function can be chosen via an appropriate selection of the system parameters [9], [10].

Differential game theory analyzes strategic interactions between competing agents, providing a powerful framework for addressing robust optimal control problems. Specifically, the disturbance rejection control problem in $\mathcal{H}_\infty$ control theory [5], [11], [12] can be formulated as a *two-player zero-sum game* wherein the controller is a minimizing player and the disturbance is a maximizing player. Infinite-horizon zero-sum games for linear and nonlinear dynamical systems with quadratic and nonquadratic performance measures are studied in [13]–[19]. In particular, sufficient conditions are provided to characterize a saddle point solution for the game and closed-loop system asymptotic, partial-state asymptotic, and partial-state finite-time stability in [16]–[18]. In light of the above, although these game-theoretic control frameworks establish stability and Nash equilibrium, predefined-time stability is *not* ensured, and safety is *not* a design consideration.

Safe control theory concerns the controller analysis and synthesis for a safety critical dynamical system to guarantee the satisfaction of safety specifications [20], which can be expressed as forward invariance [3] of a set of safe system states. *Control barrier functions* (CBF) have been commonly used to guarantee the safety of a control system by rendering a safe set forward invariant [21]–[23]. The problem of *asymptotic* stabilization with guaranteed safety is addressed

[1]N.-M. T. Kokolakis and R. Mangharam are with the Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia, PA 19104, USA. E-mail: {nmkoko, rahulm}@seas.upenn.edu.

[2]S. Liu, J. Darbon, and G. E. Kaniadakis are with the Division of Applied Mathematics, Brown University, Providence, RI, 02912, USA e-mail: {shanqing_liu, jerome_darbon, george_karniadakis}@brown.edu.

in [24] by merging a control Lyapunov function (CLF) [25] and a CBF [21]. However, a CLBF cannot exist, as shown in [26]. Alternatively, quadratic programming (QP) has been utilized to combine a CLF and a CBF to synthesize controllers for safe *asymptotic* stabilization of nonlinear systems [27], [28]. A key limitation of these frameworks is the lack of robustness guarantees. In contrast, building on the results of [29], the notion of robust CBF is introduced in [30] to construct controllers for nonlinear systems with exogenous disturbances that guarantee safety and input-to-state stability [3]. However, CBF-based QPs introduce undesirable *asymptotically* stable equilibria [31], do not optimize closed-loop system performance in the face of a worst-case adversary, and do not enforce time constraints. To the best of our knowledge, a game-theoretic control framework that *simultaneously* ensures *safety*, *predefined-time stability*, *optimality*, and *robustness* is absent from the literature.

To synthesize the Nash equilibrium strategies for a zero-sum differential game formulating a robust optimal stabilization problem, it is first necessary to determine the value of the game, which is a *stabilizing* solution of a nonlinear partial differential equation, the steady-state Hamilton–Jacobi–Isaacs (HJI) equation. Solving the steady-state HJI equation is generally intractable, except for special cases [32]. *Physics-informed neural networks* (PINNs), first developed in [33], have demonstrated their effectiveness in approximating a stabilizing solution to the steady-state Hamilton–Jacobi–Bellman (HJB) equation related to an *optimal stabilization problem* [34]–[36]. However, using PINNs to solve a zero-sum differential game has *not* been explored. To the best of our knowledge, the literature lacks a game-theoretic physics-informed learning framework that approximates the unique stabilizing solution to the steady-state HJI.

Contributions: The contributions of this paper are threefold. First, we address an adversarially robust optimal safe predefined-time stabilization problem formulated as a two-player zero-sum differential game. Second, sufficient conditions for the existence of a saddle-point solution to the zero-sum game and closed-loop system safe predefined time stability are derived in terms of a barrier Lyapunov function. Finally, an *adversarial physics-informed learning* algorithm is developed to learn the solution to the robust optimal safe predefined-time stabilization problem.

II. Robust Optimal Safe Predefined-Time Stabilization

In this section, we formulate the robust optimal safe predefined time stabilization problem as a *two-player zero-sum differential game* to characterize robust optimal feedback controllers that render the equilibrium point of the closed-loop system safely predefined-time stable while optimizing the closed-loop system performance against the worst-case feedback adversary. Specifically, we provide sufficient conditions for the existence of a safely predefined time stabilizing feedback *Nash equilibrium* solution to the zero-sum game.

Consider the parameter-dependent nonlinear affine dynamical system given by

$$\dot{x}(t) = f(x(t),\theta_f) + G(x(t),\theta_G)u(t) + K(x(t),\theta_K)a(t), \quad x(0) = x_0, \quad t \geqslant 0, \tag{1}$$

where, for every $t \geqslant 0$, $x(t) \in \mathbb{R}^n$ is the state vector, $u(t) \in \mathbb{R}^{m_u}$ is the control input, $a(t) \in \mathbb{R}^{m_a}$ is the adversarial input, $f : \mathbb{R}^n \times \mathbb{R}^{N_f} \to \mathbb{R}^n$ is such that $f(\cdot,\theta_f)$ is continuous on $\mathbb{R}^n$ for all $\theta_f \in \mathbb{R}^{N_f}$ and $f(0,\cdot) = 0$, $G : \mathbb{R}^n \times \mathbb{R}^{N_G} \to \mathbb{R}^{n\times m_u}$ is such that $G(\cdot,\theta_G)$ is continuous on $\mathbb{R}^n$ for all $\theta_G \in \mathbb{R}^{N_G}$, and $K : \mathbb{R}^n \times \mathbb{R}^{N_K} \to \mathbb{R}^{n\times m_a}$ is such that $K(\cdot,\theta_K)$ is continuous on $\mathbb{R}^n$ for all $\theta_K \in \mathbb{R}^{N_K}$.

Let $\mathcal{S} \subset \mathbb{R}^n$ be a set of *admissible states* with $0 \in \mathcal{S}$ and let $T_{\rm p} > 0$ be a *predefined time*. To evaluate the performance of the controlled parameter-dependent nonlinear dynamical system (1), we define the performance measure

$$J\left(x_0, u(\cdot), a(\cdot)\right) = \int_0^{T_{\rm p}} \Big(L(x(t)) + L_u(x(t))u(t) + L_a(x(t))a(t) + u^{\rm T}(t)R_u(x(t))u(t) - a^{\rm T}(t)R_a(x(t))a(t)\Big){\rm d}t, \tag{2}$$

where $L : \mathcal{S} \to \mathbb{R}$, $L_u : \mathcal{S} \to \mathbb{R}^{1\times m_u}$, $L_a : \mathcal{S} \to \mathbb{R}^{1\times m_a}$, $R_u : \mathcal{S} \to \mathbb{R}^{m_u\times m_u}$, and $R_a : \mathcal{S} \to \mathbb{R}^{m_a\times m_a}$ are continuous on $\mathcal{S}$ such that $L(0) = 0$, $L_u(0) = 0$, $L_a(0) = 0$, $R_u(x) > 0,\ x \in \mathcal{S}$, and $R_a(x) > 0,\ x \in \mathcal{S}$. Note that $L(\cdot)$ penalizes deviations of the state x from the origin, if $L(x) \geqslant 0,\ x \in \mathcal{S}$, $L_u(\cdot)$ penalizes alignment with the control input u, $L_a(\cdot)$ rewards alignment with the adversary input a, and $R_u(\cdot)$ and $R_a(\cdot)$ penalize control and adversary effort. The controller $u(\cdot)$ is a player that *minimizes* the performance measure (2), whereas the adversary $a(\cdot)$ is a player that *maximizes* the performance measure (2).

We define, for every $x_0 \in \mathcal{S}$, the set of *safely predefined-time stabilizing pairs* of feedback strategies by $\mathcal{F}(x_0,\mathcal{S},T_{\rm p}) \triangleq \{u : [0,\infty) \to \mathbb{R}^{m_u}$ and $a : [0,\infty) \to \mathbb{R}^{m_a} : u(\cdot)$ and $a(\cdot)$ are a feedback control strategy and a feedback adversary strategy and $x(t),\ t \geqslant 0$, is a solution to (1) satisfying $x(t) \in \mathcal{S}$ for all $t \geqslant 0$ and $x(t) = 0$ for all $t \geqslant T_{\rm p}\}$. Furthermore, let $\mathcal{F}_u(x_0,\mathcal{S},T_{\rm p})$ and $\mathcal{F}_a(x_0,\mathcal{S},T_{\rm p})$ be the sets of feedback control strategies and feedback adversary strategies such that $\mathcal{F}_u(x_0,\mathcal{S},T_{\rm p}) \times \mathcal{F}_a(x_0,\mathcal{S},T_{\rm p}) = \mathcal{F}(x_0,\mathcal{S},T_{\rm p})$.

The next theorem gives sufficient conditions for the existence of a safely predefined time stabilizing feedback *Nash equilibrium* solution to the two-player zero-sum game.

Theorem 1: Consider the parameter-dependent nonlinear affine dynamical system (1) with performance measure (2). Assume that there exist a continuously differentiable function $V : \mathcal{S} \to \mathbb{R}$, system parameter vectors $\theta_f \in \mathbb{R}^{N_f}$, $\theta_G \in \mathbb{R}^{N_G}$, and $\theta_K \in \mathbb{R}^{N_K}$, and real numbers $\alpha,\ \beta,\ p,\ q,\ k > 0$ such that $pk < 1,\ qk > 1$, and

$$L(x) + V'(x)f(x,\theta_f) - \frac{1}{4}\Big[V'(x)G(x,\theta_G) + L_u(x)\Big] \cdot R_u^{-1}(x)\Big[V'(x)G(x,\theta_G) + L_u(x)\Big]^{\rm T}$$

$$+\frac{1}{4}\Big[V'(x)K(x,\theta_K)+L_a(x)\Big]$$

$$\cdot R_a^{-1}(x)\Big[V'(x)K(x,\theta_K)+L_a(x)\Big]^{\mathrm{T}}=0,\quad x\in\mathcal{S},\tag{3}$$

$$V(0)=0,\tag{4}$$

$$V(x)>0,\quad x\in\mathcal{S}\backslash\{0\},\tag{5}$$

$$V(x)\to\infty \text{ as } x\to\partial\mathcal{S},\tag{6}$$

$$\begin{aligned}V'(x)\Big[&f(x,\theta_f)-\frac{1}{2}G(x,\theta_G)R_u^{-1}(x)L_u^{\mathrm{T}}(x)\\&+\frac{1}{2}K(x,\theta_K)R_a^{-1}(x)L_a^{\mathrm{T}}(x)\\&-\frac{1}{2}G(x,\theta_G)R_u^{-1}(x)G^{\mathrm{T}}(x,\theta_G)V'^{\mathrm{T}}(x)\\&+\frac{1}{2}K(x,\theta_K)R_a^{-1}(x)K^{\mathrm{T}}(x,\theta_K)V'^{\mathrm{T}}(x)\Big]\\&\leqslant-\frac{\gamma}{T_{\mathrm{p}}}\left(\alpha V^p(x)+\beta V^q(x)\right)^r,\quad x\in\mathcal{S},\end{aligned}\tag{7}$$

where

$$\gamma\triangleq\frac{\Gamma\left(\frac{1-kp}{q-p}\right)\Gamma\left(\frac{kq-1}{q-p}\right)}{\alpha^k\Gamma(k)(q-p)}\left(\frac{\alpha}{\beta}\right)^{\frac{1-kp}{q-p}}.$$

If either $\mathcal{S}$ is bounded or both $\mathcal{S}$ is unbounded and $V(\cdot)$ is coercive, then there exists a control parameter vector $\theta_{\mathrm{c}}\in\mathbb{R}^{N_{\mathrm{c}}}$ and an adversary parameter vector $\theta_{\mathrm{a}}\in\mathbb{R}^{N_{\mathrm{a}}}$ such that with the feedback control strategy

$$\begin{aligned}u(t)=&u^\star(x(t),\theta_{\mathrm{c}})\\\triangleq&-\frac{1}{2}R_u^{-1}(x(t))\big[L_u(x(t))+V'(x(t))G(x(t),\theta_G)\big]^{\mathrm{T}},\\&\qquad x(t)\in\mathcal{S},\quad t\geqslant 0,\end{aligned}\tag{8}$$

and the feedback adversary strategy

$$\begin{aligned}a(t)=&a^\star(x(t),\theta_{\mathrm{a}})\\\triangleq&\frac{1}{2}R_a^{-1}(x(t))\big[L_a(x(t))+V'(x(t))K(x(t),\theta_K)\big]^{\mathrm{T}},\\&\qquad x(t)\in\mathcal{S},\quad t\geqslant 0,\end{aligned}\tag{9}$$

the zero solution $x(t)\equiv 0$ to (1) is safely predefined-time stable with predefined time T_{p} with respect to the set of admissible states $\mathcal{S}$. Furthermore, if $x_0\in\mathcal{S}$, then the pair of feedback strategies $(u^\star(\cdot),a^\star(\cdot))$ is the Nash equilibrium of the two-player zero-sum game in the sense that

$$\begin{aligned}&J(x_0,u^\star(x(\cdot),\theta_{\mathrm{c}}),a^\star(x(\cdot),\theta_{\mathrm{a}}))\\&=\min_{u(\cdot)\in\mathcal{F}_u(x_0,\mathcal{S},T_{\mathrm{p}})}\max_{a(\cdot)\in\mathcal{F}_a(x_0,\mathcal{S},T_{\mathrm{p}})}J\left(x_0,u(\cdot),a(\cdot)\right)\\&=\max_{a(\cdot)\in\mathcal{F}_a(x_0,\mathcal{S},T_{\mathrm{p}})}\min_{u(\cdot)\in\mathcal{F}_u(x_0,\mathcal{S},T_{\mathrm{p}})}J\left(x_0,u(\cdot),a(\cdot)\right)\end{aligned}$$

and the Nash value is

$$J(x_0,u^\star(x(\cdot),\theta_{\mathrm{c}}),a^\star(x(\cdot),\theta_{\mathrm{a}}))=V(x_0).$$

Proof. The proof is given in [37]. ■

The *robust optimal safe predefined-time stabilization* problem is equivalent to solving the steady-state HJI equation (3) subject to the constraints (4)–(7), which is generally difficult to solve, except for special cases. In the next section, we present learning-based techniques for approximating the solution of the HJI equation.

III. PINNs for robust optimal safe control

In this section, building on the results of [38], we design a *physics-informed learning* framework to approximate the safely predefined-time stabilizing solution $V(\cdot)$ of the steady-state HJI equation (3). Specifically, invoking the universal approximation property of deep neural networks [39], we introduce a surrogate model $\hat{V}(\cdot,w)$ with $w\in\mathbb{R}^N$ representing the trainable model parameters. To ensure the satisfaction of the constraints (4)–(6), let

$$\hat{V}(x,w)=h(V_{\mathrm{NN}}(x,w))B(x),\quad (x,w)\in\mathcal{S}\times\mathbb{R}^N,\tag{10}$$

where $h:\mathbb{R}\to(0,\infty)$ is a user-defined continuously differentiable function, $V_{\mathrm{NN}}:\mathcal{S}\times\mathbb{R}^N\to\mathbb{R}$ is a standard fully-connected neural network, and $B:\mathcal{S}\to\mathbb{R}$ is a user-defined continuously differentiable function satisfying $B(0)=0$, $B(x)>0$, $x\in\mathcal{S}\backslash\{0\}$, and $B(x)\to\infty$ as $x\to\partial\mathcal{S}$. If $\mathcal{S}$ is unbounded, then $B(\cdot)$ is additionally coercive.

To learn an approximation $\hat{V}(\cdot,w)$ of $V(\cdot)$, we randomly sample M points in $\mathcal{S}$ and let $S_{\mathrm{col}}\triangleq\{x_1,\ldots,x_M\}\subset\mathcal{S}$ denote the set of *collocation points*. The learning procedure is formulated as a *constrained* optimization problem, where, at the collocation points, the loss function $\mathcal{E}(\cdot)$ penalizes violations of the steady-state HJI equation (3) and the constraint function $l(\cdot,\cdot)$ enforces the differential inequality (7) to guarantee safe predefined-time stability. Specifically, the constrained optimization problem is of the form

$$\begin{aligned}&\min_{w\in\mathbb{R}^N}\mathcal{E}(w)\\&\text{subject to } l(x,w)\leqslant 0,\quad x\in S_{\mathrm{col}},\end{aligned}\tag{11}$$

where the loss function $\mathcal{E}(\cdot)$ and the constraint function $l(\cdot,\cdot)$ are defined by

$$\begin{aligned}\mathcal{E}(w)\triangleq\sum_{x\in S_{\mathrm{col}}}\Big|&L(x)+\hat{V}_x(x,w)f(x,\theta_f)\\&-\frac{1}{4}\left(\hat{V}_x(x,w)G(x,\theta_G)+L_u(x)\right)\\&\cdot R_u^{-1}(x)\left(\hat{V}_x(x,w)G(x,\theta_G)+L_u(x)\right)^{\mathrm{T}}\\&+\frac{1}{4}\left(\hat{V}_x(x,w)K(x,\theta_K)+L_a(x)\right)\\&\cdot R_a^{-1}(x)\left(\hat{V}_x(x,w)K(x,\theta_K)+L_a(x)\right)^{\mathrm{T}}\Big|^2,\\&\qquad w\in\mathbb{R}^N,\end{aligned}\tag{12}$$

and

$$\begin{aligned}l(x,w)\triangleq\hat{V}_x(x,w)\Big(&f(x,\theta_f)-\frac{1}{2}G(x,\theta_G)R_u^{-1}(x)L_u^T(x)\\&+\frac{1}{2}K(x,\theta_K)R_a^{-1}(x)L_a^T(x)\\&-\frac{1}{2}G(x,\theta_G)R_u^{-1}(x)G^T(x,\theta_G)\hat{V}_x^T(x,w)\end{aligned}$$

$$+ \frac{1}{2} K(x, \theta_K) R_a^{-1}(x) K^T(x, \theta_K) \hat{V}_x^T(x, w)\Big) + \frac{\gamma}{T_p}\Big(\alpha \hat{V}^p(x, w) + \beta \hat{V}^q(x, w)\Big)^r, \quad (x, w) \in \mathcal{S}_{\text{col}} \times \mathbb{R}^N. \quad (13)$$

The constrained optimization problem (11) can be numerically addressed using the *augmented Lagrangian method* (see, for example, [40] and [41]). In particular, the constrained optimization problem (11) is converted into a sequence of unconstrained optimization subproblems through an iterative procedure. In each iteration, the objective function of the unconstrained optimization subproblem is the sum of the loss function $\mathcal{E}(\cdot)$ and a penalty term for the constraints. Hence, the optimization subproblem at iteration k takes the form

$$\min_{w \in \mathbb{R}^N} \mathcal{E}_k(w), \quad (14)$$

where $\mathcal{E}_k(\cdot)$ is the loss function at iteration k given by

$$\mathcal{E}_k(w) \triangleq \mathcal{E}(w) + \sum_{x \in S_{\text{col}}} \Big(\mu_{k-1} \mathbb{1}_{\{l(x,w) \geqslant 0 \vee \lambda_{k-1}(x) > 0\}} l^2(x, w) + \lambda_{k-1}(x) l(x, w)\Big), \quad (15)$$

with $\vee$ representing the or operator.

For every iteration $k \in \mathbb{Z}_+$, the Lagrangian multipliers μ_k and $\lambda_k(\cdot)$ in (15) are updated as

$$\mu_k = \delta \mu_{k-1}, \quad (16)$$

$$\lambda_k(x) = \max\{0, \lambda_{k-1}(x) + 2\mu_{k-1} l(x, w)\}, \; x \in S_{\text{col}}, \quad (17)$$

with $\delta, \; \mu_0 \in \mathbb{R}$ being tunable hyperparameters, and $\lambda_0(x)$ is initialized to be 0 for every $x \in S_{\text{col}}$. The optimization subproblem (14) can be solved using modern gradient-based or (quasi-) Newton-based numerical solvers, such as Adam [42] or L-BFGS [43].

Let w_k denote the minimizer of the optimization subproblem (14) at iteration k. Substituting w_k into (10) yields $\hat{V}(\cdot, w_k)$, an approximation of the value function. Furthermore, substituting $\hat{V}(\cdot, w_k)$ into (8) and (9) yields the approximate Nash feedback control and adversary strategies $\hat{u}(\cdot, w_k)$ and $\hat{a}(\cdot, w_k)$, respectively. Algorithm 1 presents the pseudocode for the proposed adversarial physics-informed learning framework for robust optimal safe control, executed for a given number of iterations $\mathcal{K}$. The architecture of Algorithm 1 is shown in Fig. 1.

Remark 1: Note that the steady-state HJI equation (3) may have multiple solutions. However, the Nash value $V(\cdot)$ is the unique safely predefined-time stabilizing solution. Hence, when using PINNs to solve the robust optimal safe predefined-time stabilization problem, enforcing the stability conditions (4)-(7) is imperative. Conditions (4)-(6) are satisfied by the design of the PINN architecture, while (7) is imposed as a constraint in the learning procedure. □

Simulation results are provided in Appendix.

Algorithm 1 Training procedure of Adversarial PINN

Hyperparameters: $\alpha, \beta, \gamma, T_{\text{p}}, p, q, r, \delta, \mu_0$
Input: Collocation points $S_{\text{col}} \triangleq \{x_1, \ldots, x_M\} \subset \mathcal{S}$
Output: Nash value $\hat{V}(\cdot, w_{\mathcal{K}})$
Nash equilibrium $(\hat{u}(\cdot, w_{\mathcal{K}}), \hat{a}(\cdot, w_{\mathcal{K}}))$

procedure
  $\lambda_0(x) \leftarrow 0$ for every $x \in S_{\text{col}}$
  Initialize network parameters $w_0 \in \mathbb{R}^N$
  for $k = 1 \cdots \mathcal{K}$ **do**
    $\tilde{\mathcal{E}} \leftarrow \mathcal{E}(w_{k-1})$ ▷ (12)
    $\tilde{l}(x) \leftarrow l(x, w_{k-1})$ ▷ (13)
    $\mathcal{E}_k \leftarrow \tilde{\mathcal{E}} + \sum_{x \in S_{\text{col}}} \big(\mu_{k-1} \mathbb{1}_{\{\tilde{l}(x) \geqslant 0 \vee \lambda_{k-1}(x) > 0\}} \tilde{l}^2(x) + \lambda_{k-1}(x) \tilde{l}(x)\big)$
    $w_k \leftarrow \arg\min_w \mathcal{E}_k$
    $\mu_k \leftarrow \delta \mu_{k-1}$
    $\lambda_k(x) \leftarrow \max\{0, \lambda_{k-1}(x) + 2\mu_{k-1}\tilde{l}(x)\}$ for every $x \in S_{\text{col}}$
  end for
end procedure

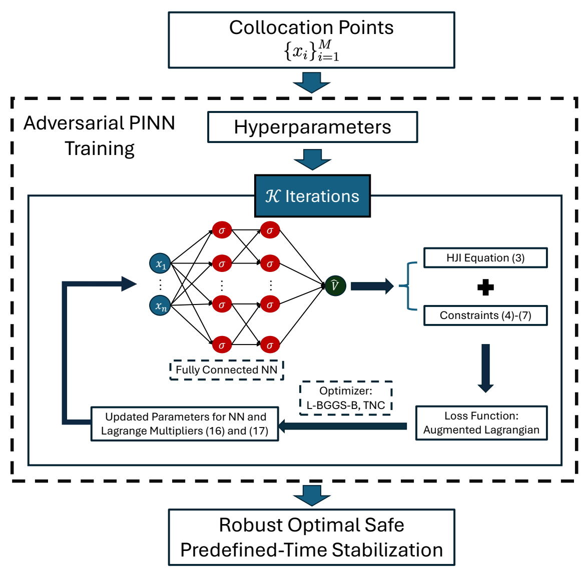

Fig. 1: Adversarial physics-informed learning architecture to solve the robust optimal safe predefined-time stabilization problem.

IV. Conclusion

In this paper, an adversarially robust optimal safe predefined-time stabilization problem is stated and shown to correspond to a two-player zero-sum differential game. Sufficient conditions are derived to characterize a safely predefined time stabilizing saddle-point solution to the differential game. Specifically, safe predefined-time stability of the closed-loop system and Nash equilibrium are established via a barrier Lyapunov function that satisfies a certain differential inequality and the steady-state HJI equation. Given the intractability of the latter, an adversarial physics-informed learning algorithm is developed to learn the safely predefined-time stabilizing solution to the steady-state HJI equation. Future research will explore discrete-time extensions of the proposed framework.

Appendix

Here, we present a numerical example to illustrate the developed robust optimal safe predefined-time control and physics-informed learning framework. Consider the nonlinear affine dynamical system given by

$$\dot{x}_1(t) = -\min\{0, x_1(t)\} + u_1(t) + a_1(t), \quad x_1(0) = x_{10}, \quad t \geqslant 0,$$

$$\dot{x}_2(t) = -\max\{0, x_2(t)\} + u_2(t) + a_2(t), \quad x_2(0) = x_{20}.$$

The set of admissible states $\mathcal{S}$ is given by $\mathcal{S} = \left\{x \in \mathbb{R}^2 : s(x) > 0\right\}$, where $s(x) \triangleq 1 - x_2^2$, $x \in \mathbb{R}^2$. Choosing

$$L(x) = \frac{1}{2}\left\| \frac{\lceil x \rfloor^{\gamma_1}}{s^{\frac{\gamma_1 - 1}{2}}(x)} + \frac{\lceil x \rfloor^{\gamma_2}}{s^{\frac{\gamma_2 - 1}{2}}(x)} \right\|_2^2 + \frac{x_1}{s(x)} \min\{0, x_1\} + \frac{x_2}{s(x)}\left(1 + \frac{\|x\|_2^2}{s(x)}\right) \max\{0, x_2\}, \quad x \in \mathcal{S},$$

$$L_u(x) = L_a(x) = \left(\frac{\lceil x \rfloor^{\gamma_1}}{s^{\frac{\gamma_1 - 1}{2}}(x)} + \frac{\lceil x \rfloor^{\gamma_2}}{s^{\frac{\gamma_2 - 1}{2}}(x)} \right)^{\mathrm{T}} - \left[\frac{x_1}{s(x)}, \ \frac{x_2}{s(x)}\left(1 + \frac{\|x\|_2^2}{s(x)}\right) \right], \quad x \in \mathcal{S},$$

$R_u(x) = \frac{1}{4} I_2$, $x \in \mathcal{S}$, and $R_a(x) = \frac{1}{2} I_2$, $x \in \mathcal{S}$, where $\gamma_1 \in (0,1)$ and $\gamma_2 > 1$, and using a similar construction as in [37] with $V(x) = \frac{\|x\|_2^2}{2s(x)}$, $x \in \mathcal{S}$, the inverse Nash equilibrium is given by

$$u^\star(x, \theta_{\mathrm{c}}) = -2\left(\frac{\lceil x \rfloor^{\gamma_1}}{s^{\frac{\gamma_1 - 1}{2}}(x)} + \frac{\lceil x \rfloor^{\gamma_2}}{s^{\frac{\gamma_2 - 1}{2}}(x)} \right), \quad x \in \mathcal{S},$$

and

$$a^\star(x, \theta_{\mathrm{a}}) = \left(\frac{\lceil x \rfloor^{\gamma_1}}{s^{\frac{\gamma_1 - 1}{2}}(x)} + \frac{\lceil x \rfloor^{\gamma_2}}{s^{\frac{\gamma_2 - 1}{2}}(x)} \right), \quad x \in \mathcal{S},$$

where $\theta_{\mathrm{c}} = \theta_{\mathrm{a}} = [\gamma_1, \ \gamma_2]^{\mathrm{T}}$.

Let $T_{\mathrm{p}} = 3.4259$ so that $\gamma_1 = 0.5$ and $\gamma_2 = 1.5$. For our PINN architecture, we let $h(x) = \frac{1}{1+e^{-x}}$, $x \in \mathbb{R}$, which is the sigmoid function, and $B(x) = \frac{\|x\|_2^2}{\sqrt{2} - \sqrt{x_2^2 + 1}}$, $x \in \mathcal{S}$. The neural network $V_{\mathrm{NN}}(\cdot, \cdot)$ is implemented as a fully connected neural network with six hidden layers, each comprising 50 neurons, using the sigmoid activation function. The number of collocation points is set to $M = 10^4$. For the augmented Lagrangian method, the hyperparameters are set to $\mu_0 = 10^{-3}$ and $\delta = 1.5$. At every iteration of Algorithm 1, the optimization subproblem (14) is solved using the truncated Newton conjugate gradient (TNCG) optimizer (see, for example, [44] and [45]).

Fig. 2 shows the approximate Nash value $\hat{V}$, the approximate Nash control strategy $\hat{u}$, and the approximate Nash adversary strategy $\hat{a}$, along with the exact Nash value V, the exact Nash control strategy $u^\star$, and the exact Nash adversary strategy $a^\star$. Note that Algorithm 1 exhibits a low symmetric absolute error (SAE). The left plot of Fig. 3 shows the closed-loop state trajectories starting from different initial conditions within the safe set $\mathcal{S}$. Note that all trajectories remain within $\mathcal{S}$ and converge to the origin. The right plot of Fig. 3 shows the time evolution of the Euclidean norm of each trajectory. Note the predefined time convergence to the origin, which verifies the settling-time function bound $T(x_0, \theta_{\mathrm{c}}, \theta_{\mathrm{a}}) \leqslant 3.4259$, $x_0 \in \mathcal{S}$.

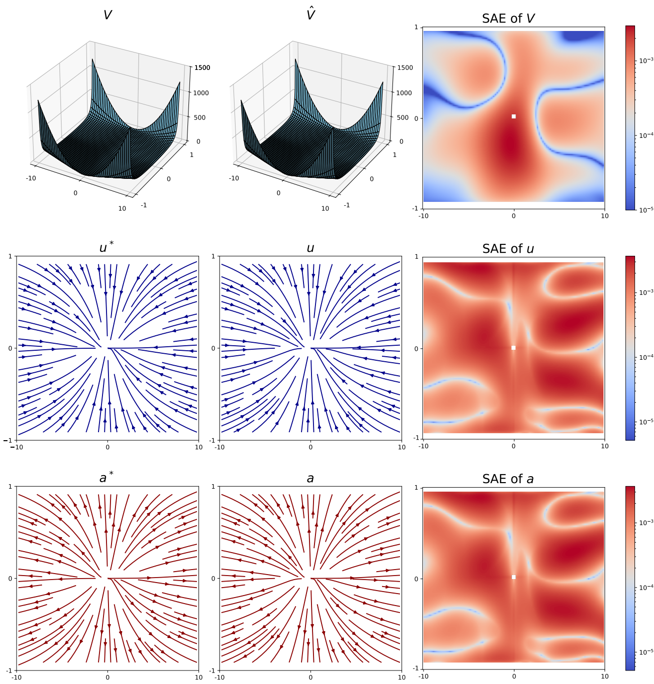

Fig. 2: Nash value, Nash feedback control strategy, and Nash feedback adversary strategy. (**Left**) Exact Nash value V, exact Nash control strategy $u^\star$, and exact Nash adversary strategy $a^\star$. (**Middle**) Approximate Nash value $\hat{V}$, approximate Nash control strategy $\hat{u}$, and approximate Nash adversary strategy $\hat{a}$. (**Right**) Symmetric absolute error for learning the Nash value, the Nash control strategy, and the Nash adversary strategy.

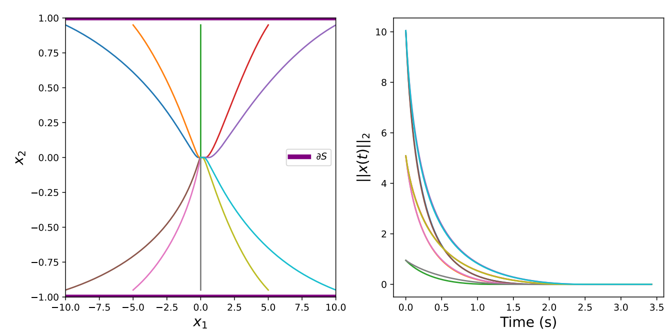

Fig. 3: Robust optimal safe predefined-time stabilization. (**Left**) Closed-loop state trajectories $x(t)$, $t \geqslant 0$, starting from different initial conditions in the safe set $\mathcal{S}$. (**Right**) Time evolution of the Euclidean norm $\|x(t)\|_2$, $t \geqslant 0$, of each trajectory shown in the left plot. In both plots, trajectories starting from the same initial condition are marked with the same color.

ACKNOWLEDGMENT

The work of N.-M.T.K. and R.M. was partially supported by US DoT Safety21 National University Transportation Center and NSF under Grant CISE-2431569. The work of S.L., J.D., and G.E.K. was partially supported by Laboratory University Collaboration Initiative (LUCI) sponsored by the Basic Research Office, Office of Under Secretary of Defense for Research and Engineering (OUSD R&E).

REFERENCES

[1] K. G. Vamvoudakis and N.-M. T. Kokolakis, *Synchronous Reinforcement Learning-Based Control for Cognitive Autonomy*. Boston - Delft: Now Publishers, 2020, vol. 8, no. 1–2.

[2] W. Xiao, C. G. Cassandras, and C. Belta, *Safe Autonomy with Control Barrier Functions: Theory and Applications*. Springer Nature, 2023.

[3] W. M. Haddad and V. Chellaboina, *Nonlinear Dynamical Systems and Control: A Lyapunov-Based Approach*. Princeton, NJ: Princeton University Press, 2011.

[4] D. Liberzon, *Calculus of Variations and Optimal Control Theory: A Concise Introduction*. Princeton, NJ: Princeton University Press, 2011.

[5] T. Başar and P. Bernhard, *H-infinity optimal control and related minimax design problems: a dynamic game approach*. Springer Science & Business Media, 2008.

[6] T. Başar and G. J. Olsder, *Dynamic noncooperative game theory*. SIAM, 1998.

[7] S. P. Bhat and D. S. Bernstein, "Finite-time stability of continuous autonomous systems," *SIAM Journal on Control and Optimization*, vol. 38, no. 3, pp. 751–766, 2000.

[8] A. Polyakov, "Nonlinear feedback design for fixed-time stabilization of linear control systems," *IEEE Transactions on Automatic Control*, vol. 57, no. 8, pp. 2106–2110, 2012.

[9] J. D. Sánchez-Torres, D. Gómez-Gutiérrez, E. López, and A. G. Loukianov, "A class of predefined-time stable dynamical systems," *IMA Journal of Mathematical Control and Information*, vol. 35, no. Supplement_1, pp. i1–i29, 2018.

[10] E. Jiménez-Rodríguez, A. J. Muñoz-Vázquez, J. D. Sánchez-Torres, M. Defoort, and A. G. Loukianov, "A lyapunov-like characterization of predefined-time stability," *IEEE Transactions on Automatic Control*, vol. 65, no. 11, pp. 4922–4927, 2020.

[11] J. A. Ball and J. Helton, "H/sup infinity/control for nonlinear plants: connections with differential games," in *Proceedings of the 28th IEEE Conference on Decision and Control,*. IEEE, 1989, pp. 956–962.

[12] A. J. van der Schaft, *Nonlinear State Space H_∞ Control Theory*. Springer, 1993.

[13] D. Jacobson, "On values and strategies for infinite-time linear quadratic games," *IEEE Transactions on Automatic Control*, vol. 22, no. 3, pp. 490–491, 1977.

[14] E. Mageirou, "Values and strategies for infinite time linear quadratic games," *IEEE Transactions on Automatic Control*, vol. 21, no. 4, pp. 547–550, 1976.

[15] D. J. Limebeer, B. D. Anderson, P. P. Khargonekar, and M. Green, "A game theoretic approach to h_∞ control for time-varying systems," *SIAM Journal on Control and Optimization*, vol. 30, no. 2, pp. 262–283, 1992.

[16] A. L'Afflitto, "Differential games, asymptotic stabilization, and robust optimal control of nonlinear systems," in *2016 IEEE 55th Conference on Decision and Control (CDC)*. IEEE, 2016, pp. 1933–1938.

[17] ——, "Differential games, continuous lyapunov functions, and stabilisation of non-linear dynamical systems," *IET Control Theory & Applications*, vol. 11, no. 15, pp. 2486–2496, 2017.

[18] ——, "Differential games, partial-state stabilization, and model reference adaptive control." *J. Frankl. Inst.*, vol. 354, no. 1, pp. 456–478, 2017.

[19] ——, "Differential games, finite-time partial-state stabilisation of nonlinear dynamical systems, and optimal robust control," *International Journal of Control*, vol. 90, no. 9, pp. 1861–1878, 2017.

[20] M. Cohen and C. Belta, *Adaptive and Learning-Based Control of Safety-Critical Systems*. Springer Nature, 2023.

[21] P. Wieland and F. Allgöwer, "Constructive safety using control barrier functions," *IFAC Proceedings Volumes*, vol. 40, no. 12, pp. 462–467, 2007.

[22] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3861–3876, 2016.

[23] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *European Control Conference*, 2019, pp. 3420–3431.

[24] M. Z. Romdlony and B. Jayawardhana, "Stabilization with guaranteed safety using control lyapunov–barrier function," *Automatica*, vol. 66, pp. 39–47, 2016.

[25] E. D. Sontag, "A 'universal'construction of artstein's theorem on nonlinear stabilization," *Systems & control letters*, vol. 13, no. 2, pp. 117–123, 1989.

[26] P. Braun and C. M. Kellett, "Comment on "stabilization with guaranteed safety using control lyapunov–barrier function"," *Automatica*, vol. 122, p. 109225, 2020.

[27] W. Ren, R. M. Jungers, and D. V. Dimarogonas, "Razumikhin and krasovskii approaches for safe stabilization," *Automatica*, vol. 146, p. 110563, 2022.

[28] P. Mestres and J. Cortés, "Optimization-based safe stabilizing feedback with guaranteed region of attraction," *IEEE Control Systems Letters*, vol. 7, pp. 367–372, 2022.

[29] X. Xu, P. Tabuada, J. W. Grizzle, and A. D. Ames, "Robustness of control barrier functions for safety critical control," *IFAC-PapersOnLine*, vol. 48, no. 27, pp. 54–61, 2015.

[30] M. Jankovic, "Robust control barrier functions for constrained stabilization of nonlinear systems," *Automatica*, vol. 96, pp. 359–367, 2018.

[31] M. F. Reis, A. P. Aguiar, and P. Tabuada, "Control barrier function-based quadratic programs introduce undesirable asymptotically stable equilibria," *IEEE Control Systems Letters*, vol. 5, no. 2, pp. 731–736, 2020.

[32] F. L. Lewis, D. Vrabie, and V. L. Syrmos, *Optimal Control*. Hoboken, NJ: John Wiley & Sons, 2012.

[33] M. Raissi, P. Perdikaris, and G. E. Karniadakis, "Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations," *Journal of Computational physics*, vol. 378, pp. 686–707, 2019.

[34] R. Furfaro, A. D'Ambrosio, E. Schiassi, and A. Scorsoglio, "Physics-informed neural networks for closed-loop guidance and control in aerospace systems," in *AIAA SCITECH 2022 Forum*, 2022, p. 0361.

[35] F. Fotiadis and K. G. Vamvoudakis, "A physics-informed neural networks framework to solve the infinite-horizon optimal control problem," in *2023 62nd IEEE Conference on Decision and Control (CDC)*. IEEE, 2023, pp. 6014–6019.

[36] N.-M. T. Kokolakis, Z. Zhang, S. Liu, K. G. Vamvoudakis, J. Darbon, and G. E. Karniadakis, "Safe physics-informed machine learning for optimal predefined-time stabilization: A lyapunov-based approach," *IEEE Transactions on Neural Networks and Learning Systems*, 2025.

[37] N.-M. T. Kokolakis, S. Liu, J. Darbon, R. Mangharam, and G. E. Karniadakis, "Adversarial physics-informed machine learning for robust optimal safe predefined-time stabilization: A game-theoretic approach," *arXiv preprint arXiv:2511.15018*, 2025.

[38] L. Lu, R. Pestourie, W. Yao, Z. Wang, F. Verdugo, and S. G. Johnson, "Physics-informed neural networks with hard constraints for inverse design," *SIAM Journal on Scientific Computing*, vol. 43, no. 6, pp. B1105–B1132, 2021.

[39] K. Hornik, M. Stinchcombe, and H. White, "Universal approximation of an unknown mapping and its derivatives using multilayer feedforward networks," *Neural Networks*, vol. 3, no. 5, pp. 551–560, 1990.

[40] J. Nocedal and S. J. Wright, *Numerical optimization*. Springer, 1999.

[41] D. P. Bertsekas, *Constrained optimization and Lagrange multiplier methods*. Academic press, 2014.

[42] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv preprint arXiv:1412.6980*, 2014.

[43] C. Zhu, R. H. Byrd, P. Lu, and J. Nocedal, "Algorithm 778: L-bfgs-b: Fortran subroutines for large-scale bound-constrained optimization," *ACM Transactions on mathematical software (TOMS)*, vol. 23, no. 4, pp. 550–560, 1997.

[44] C. T. Kelley, *Iterative methods for optimization*. SIAM, 1999.

[45] J.-F. Bonnans, J. C. Gilbert, C. Lemaréchal, and C. A. Sagastizábal, *Numerical optimization: theoretical and practical aspects*. Springer Science & Business Media, 2006.