Safety Control Synthesis with Input Limits: a Hybrid Approach

Gray C. Thomas[1], Binghan He, and Luis Sentis

***Abstract*— We introduce a hybrid (discrete–continuous) safety controller which enforces strict state and input constraints on a system—but only acts when necessary, preserving transparent operation of the original system within some safe region of the state space. We define this space using a Min-Quadratic Barrier function, which we construct along the equilibrium manifold using the Lyapunov functions which result from linear matrix inequality controller synthesis for locally valid uncertain linearizations. We also introduce the concept of a barrier pair, which makes it easy to extend the approach to include trajectory-based augmentations to the safe region, in the style of LQR-Trees. We demonstrate our controller and barrier pair synthesis method in simulation-based examples.**

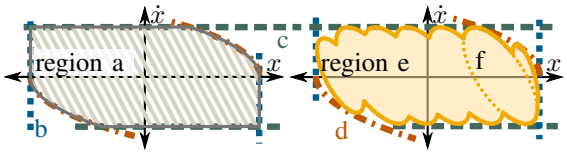

Fig. 1: The ideal safe region (a) for system $\ddot{x} = u$ with position limit (b lines), velocity limit (c lines) and acceleration or input limit (d lines). We approximate region (a) with (e), the zero sub-level set of our min-Quadratic barrier function, which is a union of robustly invariant ellipsoids (f) centered about various points on the equilibrium manifold.

I. Introduction

Controllers which ensure safe operation of dynamic systems despite un-trusted inputs are widely appreciated for their straightforward safety verification. They find application where safety is critical, and also where input foresight is unavailable. These systems must first guarantee future satisfaction of both state and input constraints on the dynamic system—with input limits being a critical complicating factor. As was famously argued in the first Bode lecture, input limits on the fuel rod controller explain the signal behavior minutes before the Chernobyl reactor's nuclear melt-down [1]. A natural secondary goal is to maximize the region of the state space that the controller certifies as safe to use.

Unlike the reference governor [2], which enforces state constraints by way of constrained model predictive control [3], safety controllers for nonlinear systems use the sub-level sets of a scalar function—a Lyapunov function, or one of several relaxations—to encode information about the safe region boundary.

Several barrier Lyapunov nonlinear approaches start by building a Lyapunov function which is infinite within the unsafe region. Backstepping [4] and adaptive control techniques [5] can then guarantee safety, if not input limits. Less restrictive barrier functions and barrier certificates must decrease only at the boundary [6]—the sub-level set of zero. Barrier Lyapunov functions can be constructed from a Lyapunov function and a barrier function [7], but finding such functions is the classical art of nonlinear control practitioners.

A control Lyapunov function [8] merely needs to be capable of decreasing everywhere, and control barrier functions [9] relax limitations on the choice of scalar function to the utmost—but still leaves the construction of such functions, and the bounding of the input, as an art. The secondary, or non-safety control objectives can be combined into a composite function [10], or added to the optimization which determines the input [7], [11], [12], but doing so alters the original controller's behavior everywhere. In particular, [11] and [12] emphasize that high relative order constraints require careful adjustments to the boundary function to avoid large inputs.

Automatic synthesis of barrier certificates through sum of squares (SoS) optimization [13] has emerged as the standard solution to this design-burden issue, and has been adopted in safety verification [14], and region of attraction estimation [15] for already designed controllers in the presence of constraints. Most ambitiously, the LQR-Tree algorithm [16], [17] attempts to map out the entire backwards-reachable state space using the union of funnels—the sub-level sets of trajectory tracking LQR Lyapunov functions. The LQR-Tree strategy could potentially be adapted to safety control, but remains structurally plagued by the non-conservative polynomial approximation of the dynamics, inability to exploit choices available during controller design, and—despite efforts to improve the speed by sacrificing guarantees [18]—dimensional explosion of the SoS sub-problem, trajectory optimization sub-problem, and the tree structure in the full state space [17].

Linear matrix inequality (LMI) controller synthesis problems (c.f. [19]) offer a conservative way to certify invariant ellipsoids as safe—and design controllers to maximize their area. Such invariant ellipsoids have been applied to input and state constrained linear systems [20], and it has been shown that under these conditions the convex hull of the regions is also invariant. But the these ellipsoids must share the same center. The less-explored, non-convex min-quadratic function mentioned in [21] for same-center ellipsoids—which bears similarity to the minimization over quadratics that runs once to select the starting funnel in [18]—is more easily adapted

This work was supported by NASA Space Technology Research Fellowship NNX15AQ33H (G.C.T), and a Longhorn Innovation Fund For Technology grant (B.H.). [1]gray.c.thomas@utexas.edu. Authors are with The Departments of Mechanical Engineering (G.C.T., B.H.) or Aerospace Engineering (L.S.), University of Texas at Austin, Austin, TX 78712-0292, USA.

to our purpose.

In this paper we propose to use linear differential inclusions to approximate a nonlinear system at a grid of equilibriums—each a conservative approximation of the nonlinear model within some region of validity. For each equilibrium we use an LMI to find the linear feedback and quadratic Lyapunov function such that the function's unity-sublevel set satisfies all state and input constraints while certifying the largest volume region. Our min-quadratic barrier function is the minimum over all of these quadratic Lyapunov functions—minus one so that the 0-sub-level set is an approximation of the safe region. This produces an approximate safe region which is the union of ellipsoids, region e in Fig. 1.

The ideal safety controller, in our view, would adhere exactly to Fig. 1's region (a), applying either no input, or limit-saturated input as soon as the state hits the boundary of the safe region. This strategy relies on being able to compute this region, but this is only feasible in SISO systems of order less than 2, in which case the safety boundary can be found by a series of integrations [22], [23], [24].

We use two slightly negative "threshold" level sets of the min-quadratic barrier function to engage and disengage the safety controller—which applies the equilibrium-centered linear feedback law associated with the current minimum over the Lyapunov functions when active. When the state reaches the first (greater) threshold, the controller activates, applies a control input guaranteed to reduce the active Lyapunov function, and thus reduces the min-quadratic barrier function itself. This continues until the min-quadratic barrier function falls below the second (lower) threshold, and the system returns to transparent operation. Trajectories which stay within the larger of the two threshold level sets are thus unaffected by the safety control.

We demonstrate our technique by constructing the region in which an inverted pendulum can balance, subject to speed and tight input limits—demonstrating the natural emergence of an exponential deceleration limit near the point where the force of gravity overwhelms the pendulum. We also simulate the high relative order behavior of a series elastic actuator under position and motor effort constraints.

II. Preliminaries

A. Problem Statement

We consider the problem of designing a safety controller $\mathbf{K}$ and safe region $\mathcal{X}_0$ for the system Σ_0:

$$\dot{x} = f(x) + g(x)u \tag{1}$$

which forms a safe closed loop system Σ_s, guaranteed to satisfy constraints $x \in \mathcal{X}$ and $u \in \mathcal{U}$ indefinitely, for all initial states in $\mathcal{X}_0 \subseteq \mathcal{X}$.

B. Barrier Pairs

Since we have input constraints, we define a concept to stand in for the standard notion of barrier functions.

Definition 1: A *Barrier Pair* is a pair of functions $(B,\ k)$ with two properties: invariance and constraint satisfaction;

$$-1 < B(x) \leq 0, u = k(x) \implies \dot{B}(x) < 0, \tag{2}$$

$$B(x) \leq 0 \implies x \in \mathcal{X},\ k(x) \in \mathcal{U}. \tag{3}$$

Note that this definition is more stringent than a barrier function, since not only B but also $B-\epsilon\ \forall\ 0 \geq \epsilon > -1$ must be a barrier function for the system $\dot{x} = f(x) + g(x)k(x)$. Additionally, while barrier functions can be expected to hold for a saturated-input system, they do not themselves uphold limits on the inputs. These requirements on B also impose a constraint which is not present in (nor particularly convenient to include in) the definition of control barrier functions, that

$$\min_{u\in\mathcal{U}} \dot{B}(x) < 0 \quad \forall\ x \in \{x : B(x) \leq 0\}. \tag{4}$$

Barrier pairs permit a (discontinuous) version of [9]'s Theorem 7 with a claim on the input bound:

Proposition 1: Given system Σ_0, a barrier pair (B, k), and a partially known policy, for any $0 \geq \epsilon > -1$

$$k_0(x) = \begin{cases} k(x) & B(x) = \epsilon \\ u \in \mathcal{U} & \text{otherwise} \end{cases} \tag{5}$$

then if $\mathbf{K}$ implements $u = k_0(x)$, Σ_s is safe and $\mathcal{X}_0$ can be chosen

$$\mathcal{X}_0 = \{x\ :\ B(x) \leq \epsilon\} \tag{6}$$

Proof: $B(x) = \epsilon \implies u = k(x) \implies \dot{B}(x) < 0,\ \therefore \mathcal{X}_0$ is invariant, $x \in \mathcal{X}_0 \implies B(x) \leq \epsilon \implies x \in \mathcal{X},\ k_0(x) \in \mathcal{U}$. ∎

The lower bound on $B(x)$ in the invariance condition (2) allows for Lyapunov functions, which do not decrease at the origin—or which, in some uncertain systems, do not decrease inside the boundary of a residual set—to be used in a barrier pair (after some minor shifting and scaling).

C. Barrier Pair LMI Subproblem

Consider a linear differential inclusion (LDI) model [19] which approximates Σ_0 near an equilibrium[1]—a robust linearization. We will focus on polytopic LDIs[2]

$$\dot{x} \in \mathbf{Co}\{A_l(x - x_e) + B_l(u - u_e),\ l = 1, \ldots, L\}, \tag{7}$$
$$\forall\quad x \in \{x\ :\ |a_i^T(x - x_e)| \leq \alpha_i,\ i = 1, \ldots, n_a\} \subseteq \mathcal{X},$$
$$u \in \{u :\ |b_i^T(u - u_e)| \leq \beta_i,\ i = 1, \ldots, n_b\} \subseteq \mathcal{U},$$

operator $\mathbf{Co}$ denoting convex hull, which approximate Σ_0 near an equilibrium $(x_e,\ u_e)\ :\ f(x_e) + g(x_e)u_e = 0$.

This allows a fairly standard set of LMI constraints to determine a positive definite matrix Q, and full state feedback matrix K such that—defining scalar $B(x) \triangleq (x - x_e)^T Q^{-1}(x - x_e) - 1$ and ellipsoidal region $\mathcal{E} \triangleq \{x \mid B(x) \leq 0\}$—when $u = k(x) \triangleq u_e + K(x - x_e)$ and $x \in \mathcal{E}$,

[1]Generating robust approximations does not have an easy catch-all solution, but is often possible with a little insight into the problem structure. While simply adding model conservatism is another option, we advise a rigorous empirical validation if the safety guarantees are important.

[2]This is for simplicity; the norm-bounded LDI has the best scaling for high dimensional problems.

then $B(x)+1$ is a Lyapunov function, x satisfies all state constraints, and u satisfies all input constraints.

Following the standard trick [19] to make this type of problem convex, we define $Y \triangleq KQ$ as an optimization variable—and extract K from Y and Q after the problem is solved.

State constraints from (7) are enforced such that $x \in \mathcal{E} \implies |a_i^T(x-x_e)| < \alpha_i$—a linear constraint on Q

$$a_i^T Q a_i \leq \alpha_i^2. \tag{8}$$

And input constraints in the form

$$\begin{pmatrix} Q & Y^T b_i \\ b_i^T Y & \beta_i^2 \end{pmatrix} \succeq 0. \tag{9}$$

are added to ensure $x \in \mathcal{E} \implies |b^T(k(x)-u_e)| \leq \beta_i$. To guarantee $B(x) < 0,\ u = k(x) \implies \dot{B}(x) < 0$ is equivalent to the standard Lyapunov condition,

$$A_l Q + Q A_l^T + B_l Y + Y^T B_l^T \prec 0 \ \forall\ l = 1, \ldots, L. \tag{10}$$

And finally, to maximize the volume of the ellipsoid $\mathcal{E}$, we maximize the log of the determinant of Q—a concave cost function [19]. With a numerical tolerance $\varepsilon > 0$, and a minimum exponential decay rate $\lambda > 0$, our sub-problem is to

$$\begin{aligned} \underset{Q,\,Y}{\text{maximize}} \quad & \log(\det(Q)) \\ \text{subject to} \quad & Q \succeq \varepsilon I \\ & (8)\ \forall\ i = 1, \ldots, n_a \\ & (9)\ \forall\ i = 1, \ldots, n_b \\ & A_l Q + Q A_l^T + B_l Y + Y^T B_l^T + \varepsilon I + \lambda Q \preceq 0 \\ & \qquad \forall\ l = 1, \ldots, L \end{aligned} \tag{11}$$

Which naturally provides a barrier pair (B, k) if the problem is feasible.

D. Combining Barrier Pairs

Proposition 2: For any list of barrier pairs $(B_1, k_1),\ (B_2, k_2),\ \ldots,\ (B_N, k_N)$, the pair comprising the min-barrier function

$$\mathbf{B}(x) \triangleq \min_{n=1,\ldots,N} B_n(x) \tag{12}$$

and (occasionally ambiguous) control input

$$\mathbf{k}(x) \triangleq k_n(x) \mid n \in \arg\min_{n=1,\ldots,N} B_n(x), \tag{13}$$

$(\mathbf{B}, \mathbf{k})$, is also a barrier pair.

Proof: Consider the set

$$\mathcal{N} = \arg\min_{n=1,\ldots,N} B_n(x), \tag{14}$$

and in particular an $n \in \mathcal{N} : \mathbf{k}(x) = k_n(x)$. Assuming first that $-1 < \mathbf{B}(x) \leq 0$ and $u = \mathbf{k}(x)$,

$$\dot{\mathbf{B}}(x) \leq \dot{B}_n(x) < 0, \tag{15}$$

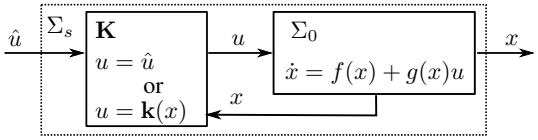

Fig. 2: Block diagram, re-purposed from [9], showing a safety controller $\mathbf{K}$ in feedback with the original system Σ_0 to produce a safe system Σ_s. The safety controller chooses either to be completely transparent ($u = \hat{u}$) or apply the known-to-be-safe input $u = \mathbf{k}(x)$.

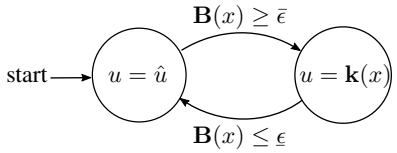

Fig. 3: Hybrid Control System

since (B_n, k_n) is a barrier pair, $u = \mathbf{k}(x) = k_n(x)$, and $-1 < \mathbf{B}(x) = B_n(x) \leq 0$. This demonstrates (2). As for (3), using the same choice of n,

$$0 \geq \mathbf{B}(x) = B_n(x) \implies x \in \mathcal{X},\ \mathbf{k}(x) = k_n(x) \in \mathcal{U} \tag{16}$$

■

We note that this combination technique is very similar to the initial funnel lookup operation in the LQR-Trees algorithm. Moreover, if they provide certain guarantees, funnels imply the existence of a barrier pair.

Proposition 3: A funnel comprising a trajectory-centered Lyapunov function $V(t,x)$ $(= V_t(x))$ and control $k(t,x)$ $(= k_t(x))$ for all $t > 0$, such that the funnel volume—the union of unity sub-level sets of $V_t\ \forall\ t > 0$—satisfies all state constraints $(V_t(x) < 1 \implies x \in \mathcal{X})$ and input constraints $(V_t(x) < 1 \implies k_t(x) \in \mathcal{U})$ guarantees the existence of a barrier pair $(\mathbf{B}, \mathbf{k})$ formed according to the following continuous parameter versions of (12) and (13):

$$\mathbf{B}(x) = \min_{t>0} V_t(x) - 1, \tag{17}$$

$$\mathbf{k}(x) = k_t(x) \mid t \in \arg\min_{t>0} V_t(x). \tag{18}$$

This pair is the combination of an infinite list of pairs $(V_t - 1, k_t)$, parameterized by a time parameter, each of which upholds constraint satisfaction (3), but does not individually have invariance (2)—unless they happen to be equilibrium-centered.

Proof: For any x inside the funnel such that $\exists\ t > 0 \mid 0 < V_t(x) \leq 1$, the funnel Lyapunov function satisfies $\dot{V} < 0$. Consider the instantaneous $t \in \arg\min_{t>0} V_t(x)$, $\mathbf{B}(x) = V_t(x) - 1$, $\mathbf{k}(x) = k_t(x)$. For an infinitesimal time $\delta > 0$,

$$\mathbf{B}(x(t+\delta)) = \min_{\tau>0} V_\tau(x(t+\delta)) - 1 \tag{19}$$

$$\leq V_{t+\delta}(x(t+\delta)) - 1 = \mathbf{B}(x) + \delta \dot{V}(t) \tag{20}$$

$$\dot{\mathbf{B}}(x) = \lim_{\delta \to 0} \frac{\mathbf{B}(x(t+\delta)) - \mathbf{B}(x)}{\delta} \leq \dot{V}(t) < 0 \tag{21}$$

Indicating that $(\mathbf{B}, \mathbf{k})$ satisfies (2). ■

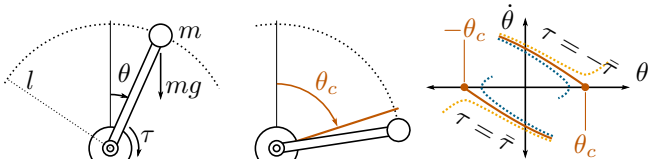

Fig. 4: Inverted pendulum model with natural position limit θ_c—a "point of no return"—due to input limit $-\bar{\tau} \leq \tau \leq \bar{\tau}$, which causes θ_c to be a critical point in the flow field for $\tau = -\bar{\tau}$ and $-\theta_c$ to be one in the flow field for $\tau = \bar{\tau}$. In our approach such points are implicitly treated as on the boundary of the unsafe set.

Note that, especially when the invariant funnel is large or the original trajectory is near to intersecting itself, applying $\mathbf{k}(x)$ is an entirely different behavior compared to applying $k(t, x)$—the barrier pair discards the information from the funnel's time parameterization.

III. Hybrid Safety Controller

Equipped with barrier pair $(\mathbf{B}, \mathbf{k})$, with its potentially non-smooth $\mathbf{k}$, we opt for an explicitly discontinuous safety controller (Fig. 2) with a simple state machine (Fig. 3) to produce hysteretic behavior—reminiscent of [6]'s second example of a safe hybrid system.

Behavior is tuned by two near-zero thresholds $\bar{\epsilon}$ and $\underline{\epsilon}$, $0 > \bar{\epsilon} > \underline{\epsilon} > -1$. As $\underline{\epsilon} \to \bar{\epsilon}$, the safety controller enforces the inequality constraint $\mathbf{B} \leq \bar{\epsilon}$, and as $\underline{\epsilon} \to -1$ it returns the system to the nearest equilibrium after each run-in with the safety limits. Detuning $\bar{\epsilon}$ from the ideal of zero can only reduce $\mathcal{X}_0$, but offers a hedge against real-world noisy signals in the computation of $\mathbf{B}(x)$.

In the examples, we use a min-quadratic barrier pair—simply the combination of those barrier pairs resulting from the LMI sub-problem. We therefore expect that applying the control $\mathbf{k}(x)$ guarantees exponential convergence to one of the equilibriums—though which one, and whether the system will transition between local control laws as it settles is not clear before hand. (This behavior is later visualized in Figs. 5 and 8.) The original equilibriums now represent the multiple minima of $\mathbf{B}$, all of them sharing the minimum value -1.

IV. Examples

In this section, we provide two simulation examples demonstrating the operation of the hybrid safety controller. The first example is a second order unstable nonlinear system, an inverted pendulum[3] (Fig. 4). The second example is a spring-mass system with 1 input and 4 states—which we use to explore the behavior near high relative-order constraints. In both examples, we use only equilibrium-centered barrier pairs—generated using our example LMI subproblem.

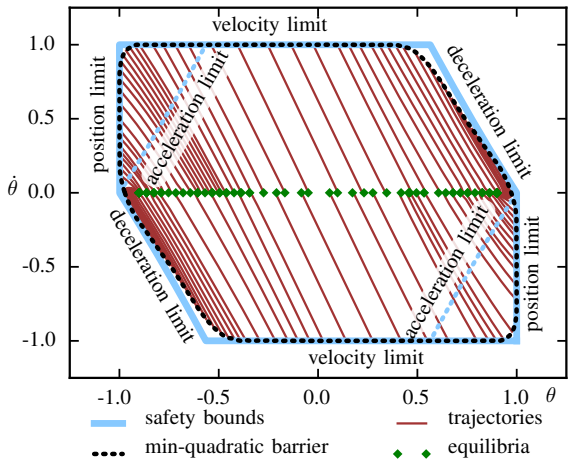

Fig. 5: Visualizing the min-quadratic approximation of the safe region with 50 ellipsoids. Acceleration limits bound reachable region, but non-reachable region can still be safe, (as starting points, for example). Simulated trajectories at the bound demonstrate behavior of under $\mathbf{k}(x)$ control.

A. Inverted Pendulum System

We consider an inverted pendulum (Fig. 4, $m = 1\text{kg}$, $l = 1.213\text{m}$, $g = 9.8\text{m/s/s}$), with safe region

$$\mathcal{X} = \left\{ \begin{bmatrix} \theta \\ \dot{\theta} \end{bmatrix} \ : \ |\theta| \leq \theta_c = 1 \text{ rad}, \ |\dot{\theta}| \leq 1 \text{ rad/s} \right\},$$
$$\mathcal{U} = \{\tau : \ |\tau| \leq \bar{\tau} = 10 \text{ N} \cdot \text{m}\}, \tag{22}$$

and dynamics

$$ml^2\ddot{\theta} = \tau + mgl \cdot \sin(\theta). \tag{23}$$

Linearizing around equilibrium θ_e, τ_e, with a validity region[4] $|\theta - \theta_e| < \alpha = \min(0.25, \theta_c - |\theta_e|)$

$$\begin{bmatrix} \dot{\theta} \\ \ddot{\theta} \end{bmatrix} \in \mathbf{Co} \left\{ \begin{bmatrix} 0 & 1 \\ \frac{g}{l} cos(\theta_e) \pm \bar{\zeta} & 0 \end{bmatrix} \begin{bmatrix} \theta - \theta_e \\ \dot{\theta} - \dot{\theta}_e \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{1}{ml^2} \end{bmatrix} (\tau - \tau_e) \right\},$$
$$\forall \quad \begin{bmatrix} \theta \\ \dot{\theta} \end{bmatrix} \in \left\{ \begin{bmatrix} \theta \\ \dot{\theta} \end{bmatrix} \ : \ |\theta - \theta_e| \leq \alpha, \ |\dot{\theta}| \leq 1 \text{ rad} \cdot \text{s}^{-1} \right\} \subseteq \mathcal{X},$$
$$\tau \in \mathcal{U},$$

where $\bar{\zeta} = \max_{\theta : |\theta - \theta_e| < \alpha} \zeta(\theta)$ represents a bound on linearization error,

$$\zeta(\theta) = \frac{g}{l} \left[\frac{sin(\theta) - sin(\theta_e)}{\theta - \theta_e} - cos(\theta_e) \right]. \tag{24}$$

While it is possible to analytically calculate this bound, it is also simple to compute via one dimensional brute force search.[5]

[3]Though others have focused on the inverted pendulum for its interesting swing-up dynamics, we imagine a pendulum for which falling is a catastrophic failure.

[4]This validity region could potentially be iteratively tuned to match the extent of the ellipse, but such concerns are of lesser importance than verifying safety. Indeed, few systems will even have a readily available function to mapping these tuned regions to trustworthy models.

[5]This is not a conservative strategy in general, but it is an extremely accurate approximation relative to the numerical tolerances in the LMI subproblem.

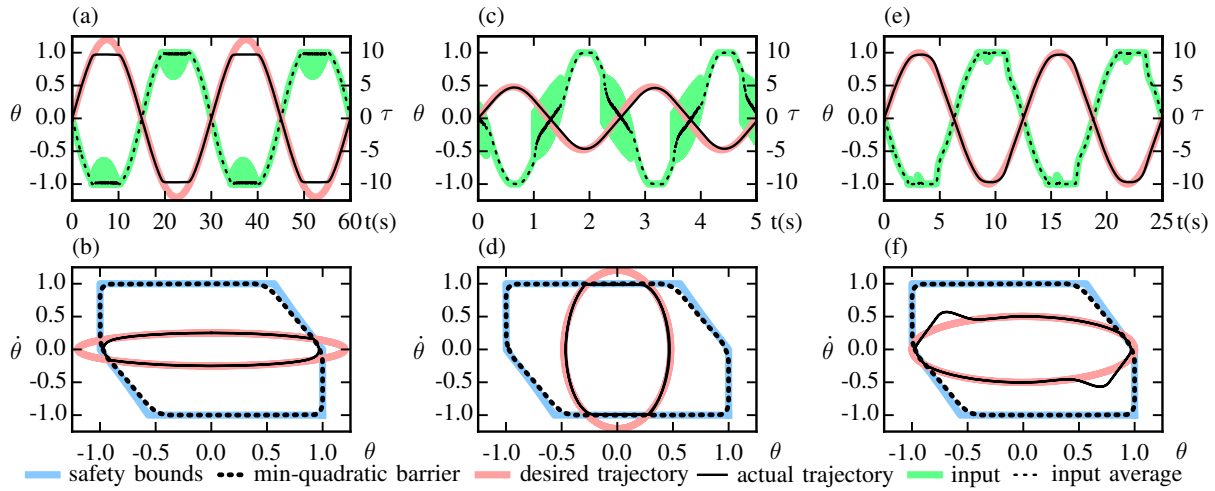

Fig. 6: The inverted pendulum system protected by the safety controller, with a low priority reference tracking task for three references—one which exceeds position bounds (a,b), one which exceeds velocity bounds (c,d) and one which would just barely push this input limited unstable system past the point of no return (e,f). Each test shown both in the time domain (a,c,e), and in the phase space (b,d,f). Chattering input signal visualized raw and with low-pass filter. Input signal in low speed (a) and (e) examples dominated by gravity bias, hence behavior mostly opposite the position. 50 equilibrium point resolution. Signal tracking after leaving $\mathbf{B}(x) = \underline{\epsilon}$ implemented with a simple feedback linearizing controller.

This brings us to the LMI subproblems: we construct 50 barrier pairs to approximate the safe region using ellipsoids (Fig. 5), and then combine them—forming a barrier pair with a min-quadratic barrier function.

In the simulation (Fig. 6), the inverted pendulum system is protected by the safety controller, with the safe system Σ_s itself in a feedback configuration with a reference tracking controller. We demonstrate the behavior using three references. For a reference exceeding position bounds (Fig. 6 a,b), the pendulum stops very close to the position bound and returns to tracking after the reference returns to $\mathcal{X}_0$. In the mean time, constraints are enforced by high speed switching. For a reference exceeding velocity bounds (Fig. 6 c,d), the pendulum stalls at the maximum allowable velocity. For a reference which would just barely push this input-limited unstable system past the point of no return (Fig. 6 e,f), the pendulum begins to rail the deceleration in advance of impact, and comes to a full stop in the safe region. When the reference returns to $\mathcal{X}_0$ it is moving relatively fast, and the reference-tracker has to exceed this speed to catch up. While this last-second deceleration behavior is not as perfect as is possible with second order systems, it is close—and this is encouraging for the higher order systems for which no equally simple policy exists.

The time plots (Fig. 6 a,c,d) show the pendulum never violates any state or input limits during the tasks. By comparing the time plots between positions and inputs, the safety controller only applies $\mathbf{k}(x)$ when it is necessary. The chattering (fast switching) of the input happens because our $\bar{\epsilon} \approx \underline{\epsilon} \approx 0$. When the pendulum is in the safety region, the performance of the reference tracking controller is preserved.

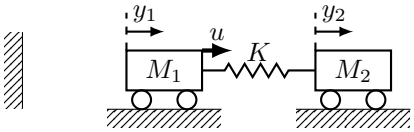

Fig. 7: A conceptual series elastic actuator model, with higher relative order constraints.

B. Double Spring-Mass

A series elastic actuator can be conceptually modeled as a dual spring-mass system (Fig 7) with M_1 as the motor, M_2 as the output inertia, and u as the motor effort ($M_1 = M_2 = 1$, $K = 1$). The safe constraints includes position limits, velocity limits, motor effort limits, and spring deflection limits:

$$\mathcal{X} = \{(y_1, \dot{y}_1, y_2, \dot{y}_2)^T : \quad |y_1 - y_2| \leq 1, \quad |y_i| \leq 1,\ |\dot{y}_i| \leq 1,\ i = 1, 2\}, \tag{25}$$

$$\mathcal{U} = \{u :\ |u| \leq 10\}.$$

A linear state equation

$$M_1 \ddot{y}_1 = K(y_2 - y_1) + u \tag{26}$$

$$M_2 \ddot{y}_2 = K(y_1 - y_2) \tag{27}$$

is valid in any point of the safe region. We use 50 barrier pairs to approximate the safe state space region.

30 trajectories are simulated on each of the 6 2D projections (Fig. 8) of the state space. These trajectories start from the edge of the min-quadratic barrier and converge to one of its 50 minima, and these projections offer a glimpse into the approximation performance of our strategy in this four dimensional space—which notably allows very tight

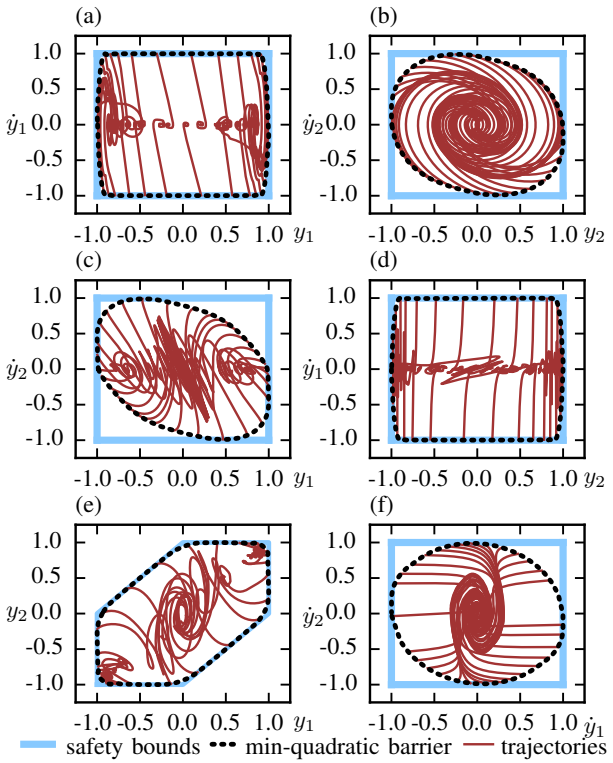

Fig. 8: Visualizing the multiple equilibriums of $\mathbf{k}$ in the series elastic actuator example. Simulated trajectories begin on the extreme-projected edge of $\mathcal{X}_0$ for each plot, and are computed separately to demonstrate the invariance of $\mathbf{B}(x) < 0$ when $u = \mathbf{k}(x)$. Ellipsoid bounds only appear to be a convex shape due to high sampling resolution along the equilibrium manifold.

adherence to the position limits in input, output, and spring deflection states.

V. Discussion

This paper presents a synthesis method for controllers that guarantee future satisfaction of all state constraints, subject to input-limited dynamics, by taking advantage of the guarantees available through LMI-based controller synthesis. We introduced the concept of barrier pairs—which make it easier to reason about the satisfaction of input limits—and a min-quadratic barrier in particular, as a simple means of combining the results of many LMI-synthesis problems. And we distinguish our work by addressing input constraints, and by synthesizing the barrier function and the controller together—so that the controller choices, which can significantly alter the shape of $B(x)$, are used to maximize its volume. It should be emphasized that in the presence of input constraints, this controller synthesis sub-problem will choose the invariant ellipse to avoid the critical points and critical-point-terminating trajectories which represent dynamic limitations due to input limits.

References

[1] G. Stein, "Respect the unstable," *IEEE Control Systems*, vol. 23, no. 4, pp. 12–25, 2003.

[2] A. Bemporad, "Reference governor for constrained nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 43, no. 3, pp. 415–419, 1998.

[3] D. Q. Mayne, J. B. Rawlings, C. V. Rao, and P. O. Scokaert, "Constrained model predictive control: Stability and optimality," *Automatica*, vol. 36, no. 6, pp. 789–814, 2000.

[4] K. P. Tee, S. S. Ge, and E. H. Tay, "Barrier Lyapunov functions for the control of output-constrained nonlinear systems," *Automatica*, vol. 45, no. 4, pp. 918–927, 2009.

[5] Y.-J. Liu and S. Tong, "Barrier Lyapunov functions-based adaptive control for a class of nonlinear pure-feedback systems with full state constraints," *Automatica*, vol. 64, pp. 70–75, 2016.

[6] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *Hybrid Systems: Computation and Control*, ser. Lecture Notes in Computer Science, 2004, vol. 2993, pp. 477–492.

[7] 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, 2017.

[8] E. D. Sontag, "A 'universal' construction of Artstein's theorem on nonlinear stabilization," *Systems & Control Letters*, vol. 13, no. 2, pp. 117–123, 1989.

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

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

[11] Q. Nguyen and K. Sreenath, "Exponential control barrier functions for enforcing high relative-degree safety-critical constraints," in *American Control Conference (ACC), 2016*. IEEE, 2016, pp. 322–328.

[12] ——, "Optimal robust safety-critical control for dynamic robotics," *International Journal of Robotics Research (IJRR), in review*, 2016.

[13] S. Prajna, "Barrier certificates for nonlinear model validation," *Automatica*, vol. 42, no. 1, pp. 117–126, 2006.

[14] A. J. Barry, A. Majumdar, and R. Tedrake, "Safety verification of reactive controllers for UAV flight in cluttered environments using barrier certificates," in *Robotics and Automation (ICRA), 2012 IEEE International Conference on*. IEEE, 2012, pp. 484–490.

[15] E. Glassman, A. L. Desbiens, M. Tobenkin, M. Cutkosky, and R. Tedrake, "Region of attraction estimation for a perching aircraft: A Lyapunov method exploiting barrier certificates," in *Robotics and Automation (ICRA), 2012 IEEE International Conference on*. IEEE, 2012, pp. 2235–2242.

[16] R. Tedrake, "LQR-trees: Feedback motion planning on sparse randomized trees," in *Robotics Science and Systems V*. MIT Press, 2009.

[17] R. Tedrake, I. R. Manchester, M. Tobenkin, and J. W. Roberts, "LQR-trees: Feedback motion planning via sums-of-squares verification," *The International Journal of Robotics Research*, vol. 29, no. 8, pp. 1038–1052, 2010.

[18] P. Reist and R. Tedrake, "Simulation-based LQR-trees with input and state constraints," in *Robotics and Automation (ICRA), 2010 IEEE International Conference on*. IEEE, 2010, pp. 5504–5510.

[19] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*. SIAM, 1994.

[20] T. Hu and Z. Lin, "Composite quadratic Lyapunov functions for constrained control systems," *IEEE Transactions on Automatic Control*, vol. 48, no. 3, pp. 440–450, 2003.

[21] T. Hu, L. Ma, and Z. Lin, "On several composite quadratic Lyapunov functions for switched systems," in *Decision and Control, 2006 45th IEEE Conference on*. IEEE, 2006, pp. 113–118.

[22] J. E. Bobrow, S. Dubowsky, and J. Gibson, "Time-optimal control of robotic manipulators along specified paths," *The International Journal of Robotics Research*, vol. 4, no. 3, pp. 3–17, 1985.

[23] G. C. Thomas and L. Sentis, "Towards computationally efficient planning of dynamic multi-contact locomotion," in *Intelligent Robots and Systems (IROS), 2016 IEEE/RSJ International Conference on*. IEEE, 2016, pp. 3879–3886.

[24] Q.-C. Pham, S. Caron, P. Lertkultanon, and Y. Nakamura, "Admissible velocity propagation: Beyond quasi-static path planning for high-dimensional robots," *The International Journal of Robotics Research*, vol. 36, no. 1, pp. 44–67, 2017.