Smooth Operator: Control Using the Smooth Robustness of Temporal Logic

Yash Vardhan Pant*, Houssam Abbas*, Rahul Mangharam
Department of Electrical and Systems Engineering
University of Pennsylvania, Philadelphia, PA, USA
{yashpant, habbas, rahulm}@seas.upenn.edu

ABSTRACT

Cyber-Physical Systems must withstand a wide range of errors, from bugs in their software to attacks on their physical sensors. Given a formal specification of their desired behavior in Metric Temporal Logic (MTL), the robust semantics of the specification provides a notion of *system robustness* that can be calculated directly on the output behavior of the system, without explicit reference to the various sources or models of the errors. The robustness of the MTL specification has been used both to verify the system offline (via robustness minimization) and to control the system online (to maximize its robustness over some horizon). Unfortunately, the robustness objective function is difficult to work with: it is recursively defined, non-convex and non-differentiable. In this paper, we propose smooth approximations of the robustness. Such approximations are differentiable, thus enabling us to use powerful off-the-shelf gradient descent algorithms for optimizing it. By using them we can also offer guarantees on the performance of the optimization in terms of convergence to minima. We show that the approximation error is bounded to any desired level, and that the approximation can be tuned to the specification. We demonstrate the use of the smooth robustness to control two quad-rotors in an autonomous air traffic control scenario, and for temperature control of a building for comfort.

1. CONTROLLING FOR ROBUSTNESS

The errors in Cyber Physical Systems (CPS) can affect both the cyber components (e.g., software bugs) and physical components (e.g., sensor failures and attacks) of a system. Under certain error models, like a bounded disturbance on a sensor reading, a CPS can be designed to be robust to that source of error. In general, however, unforeseen issues can occur. To deal with unforeseen problems, at design time, the system must be verified to be *robust* : i.e., not only does it satisfy its design specifications under the known error models, it must satisfy them robustly. Similarly, at runtime, the system's controller must make decisions that maximize this satisfaction margin, or *robustness*. This can give a margin of maneuvarability to the system during which it addresses the unforeseen problem. Since these problems are, by definition, unforeseen and unmodeled and only detected by their effect on the output, the notion of robustness must be computable using only the output behavior of the system.

*The authors contributed equally.
This work was supported by STARnet a Semiconductor Research Corporation program sponsored by MARCO and DARPA, NSF MRI-0923518 and the US Department of Transportation University Transportation Center Program.

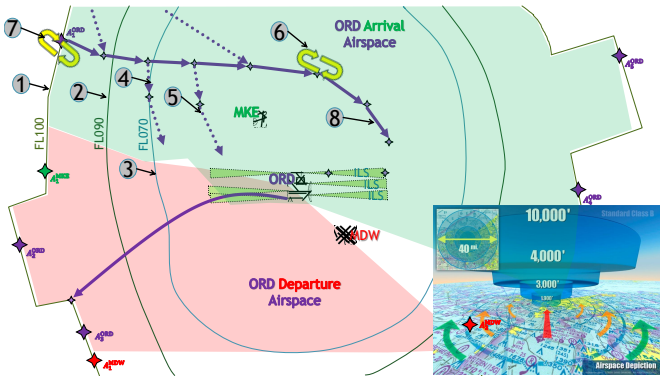


Figure 1: A simplified depiction of Chicago O'Hare (ORD) airport and its airspace (40 miles radius). The numbers indicate when and where different landing rules apply. Sub-figure on the right shows the altitude rules, see text. Figure courtesy of Max Z. Li, University of Pennsylvania.

EXAMPLE 1. *Air-Traffic Control (ATC) coordinates landing arrivals at an airport. ATCs have very complex rules to ensure that all airplanes, of different sizes and speeds, approach the airport and land safely, with sufficient margin to other airplanes to accommodate emergencies and wind gusts. Fig. 1 depicts the airspace of Chicago O'Hare (ORD), the third busiest airport in the U.S. The arrival airspace is divided into 3 zones with different, hierarchical, altitude floors and ceilings. It also shows holding zones, landing approaches, and allowable trajectories for the landing. The following is a subset of the rules that apply for incoming air-crafts.*

1. *When an aircraft enters one of the zones (indicated by the numbers 1,2,3 in Fig. 1), it must stay between that zone's altitude floor and ceiling.*
2. *If an aircraft approaches from the West, it must follow one of the trajectories numbered* 4 *or* 5.
3. *If the air-space is too busy, an aircraft must maintain a holding pattern in either holding zones* 6 *or* 7*, until some maximum amount of time expires.*
4. *A minimum separation must be maintained between aircrafts.*

How do we ensure that the ATC system satisfies these complex rules *robustly*? The *robustness of Metric Temporal Logic specifications* [12, 8] is a rigorous notion that has been used successfully for the verification of automotive systems [11, 9], medical devices [24], and general CPS. In details, MTL is a formal language for expressing complex reactive requirements with time constraints, such as those of the ATC [15]. Given a specification φ written in Metric Temporal Logic (MTL) and a system execution $\mathbf{x}$, the robustness $\rho_\varphi(\mathbf{x})$ of the spec relative to $\mathbf{x}$ measures two things: its sign tells whether $\mathbf{x}$ satisfies the spec ($\rho_\varphi(\mathbf{x}) > 0$) or falsifies it (i.e., violates it, $\rho_\varphi(\mathbf{x}) < 0$). Its magnitude $|\rho_\varphi(\mathbf{x})|$ measures how *robustly* the spec is satisfied or falsified. Namely, any perturbation to $\mathbf{x}$ of size less than $|\rho_\varphi(\mathbf{x})|$ will not cause its truth value to change. Thus, the control algorithm can *maximize* the robustness over all possible control actions to determine the next control input.

Example1, continued. *The ATC rules can be formalized in Metric Temporal Logic (MTL). Rule 1 can be formalized as follows ($\Box$ means 'Always', q is an aircraft and q_z is its altitude).*

$$\Box(q \in Zone1 \implies q_z \leq \text{Ceiling1} \wedge q_z \geq \text{Floor1}) \quad (1)$$

Rule 3 can be formalized as follows.

$$\Box(Busy \implies \Diamond_{[t_1,t_2]}(q \in \text{Holding-6} \vee q \in \text{Holding-7}) \mathcal{U}_{[0,\text{MaxHolding}]} \neg Busy) \quad (2)$$

This says that Always ($\Box$), if airport is Busy, then Eventually ($\Diamond$), sometime between times t_1 and t_2, the plane goes into a holding area. It stays there $\mathcal{U}$ntil the airport is not ($\neg$) busy, or the timer expires at time MaxHolding.

By maximizing the robusness of these MTL specifications, the ATC can automatically find landing patterns that leave room for maneuvering in case of emergencies. Any unforeseen disturbance smaller than a known bounded size will not violate the rules, and will not lead to an unsafe situation.

Unfortunately, the robustness function ρ_φ is hard to work with. It is recursively defined (does not have a closed form), and so is hard to handle analytically. It is non-convex, so optimization cannot be guaranteed to yield global optima. It is non-differentiable, so we have to resort to heuristics or costly non-smooth optimizers. Finally, it does not obey an optimality principle, so efficient Dynamic Programming algorithms cannot be used. This makes its optimization a challenge - indeed, most existing approaches treat it as a black box and apply heuristics to its optimization (see Related Work below). These heuristics provide little to no guarantees, have too many user-set parameters, and don't have rigorous termination criteria. On the other hand, *gradient descent optimization* algorithms typically offer convergence guarantees to the function's (local) minima, have known convergence rates for certain function classes, and have been optimized so they outperform heuristics that don't have access to the objective's gradient information. The existence of a gradient also allows us to do *local* search for falsifying trajectories, which is necessary for corner case bugs or dangerous situations. Moreover, gradient descent algorithms usually have a fewer number of parameters to be set by the user, and important issues like step-size selection are rigorously addressed.

Contributions. In this paper, we present smooth (infinitely differentiable) approximations to the robustness function of arbitrary MTL formulae. This allows us to run powerful and rigorous off-the-shelf gradient descent optimizers. We show that the smooth approximation is always within a user-defined error of the true robustness, and illustrate the result experimentally. We demonstrate that the resulting control algorithms, which use gradient descent on the smoothed robustness, performs better than a heuristic like Simulated Annealing optimizing the original, non-differentiable robustness. We demonstrate the results on a control case study for an autonomous airport traffic controller. Note, our method can also be applied to the falsification problem [1] by minimizing robustness.

Related work. Current approaches to optimizing the robustness fall into four categories: the use of heuristics like Simulated Annealing and RRTs [19, 2, 23, 9, 6], non-smooth optimization [3], Mixed Integer Linear Programming (MILP) [22], and iterative approximations [1, 4]. Black-box heuristics are the most commonly used approach: for example, Simulated Annealing [19], cross-entropy [23] and RRTs [9]. The clear advantage of these methods is that they do not require any special form of the objective function: they simply need to evaluate it at various points of the search space, and use its value as feedback to decide on the next point to try. A significant shortcoming is that, unlike gradient descent optimization, they offer little to no guarantees of convergence to local minima, and their convergence rates are often not known. They also use many 'magical' parameters that are heuristically set and may affect the results significantly, thus requiring more user interaction than desired. Because the robustness is non-smooth, the work in [3] developed an algorithm that decreases the objective function along its sub-gradient. This involved a series of conservative approximations, and was restricted to the case of safety formulae. In [22], the authors encoded the MTL formula as a set of linear and boolean constraints, and used an MILP solver to solve them. MILPs are NP-hard, and the sophisticated heuristics used to mitigate this make it hard to characterize their runtimes, which is important in control - see examples in [22]. The work closest to ours is [1, 4]. There, the authors considered safety formulas, for which the robustness reduces to the minimum distance between $\mathbf{x}$ and the unsafe set U. By sub-optimally focusing on one point on the trajectory $\mathbf{x}$, they replaced the objective by a differentiable indicator function for U and solved the resulting problem with gradient descent.

By computing fast smooth approximations of robustness, we circumvent most of the above issues and enable real-time control by robustness maximization.

2. ROBUSTNESS OF MTL FORMULAE

Consider a discrete-time dynamical system $\mathcal{H}$ given by

$$x_{t+1} = f(x_t, u_t) \quad (3)$$

where $x \in X \subset \mathbb{R}^n$ is the state of the system and $u \in U \subset \mathbb{R}^m$ is its control input. The system's initial state x_0 takes value from some initial set $X_0 \subset \mathbb{R}^n$. Given an initial state x_0 and a control input sequence $\mathbf{u} = (u_0, u_1, \ldots), u_t \in U$, a trajectory of the system is the unique sequence of states $\mathbf{x} = (x_0, x_1, \ldots)$ s.t. for all t, x_t is in X and it obeys (3) at every time step. We will use $\mathbb{T}$ to abbreviate the time domain $\{0, 1, 2, \ldots\}$. All temporal intervals that appear in this paper are discrete-time, e.g. $[a, b]$ means $[a, b] \cap \mathbb{T}$. For an interval I, we write $t + I = \{t + a \mid a \in I\}$. The set of subsets of a set S is denoted $\mathcal{P}(S)$. The signal space $X^{\mathbb{T}}$

is the set of all signals $\mathbf{x} : \mathbb{T} \to X$. The max operator is written $\sqcup$ and min is written $\sqcap$.

2.1 Metric Temporal Logic

The controller of $\mathcal{H}$ is designed to make the closed loop system (3) satisfy a specification expressed in Metric Temporal Logic (MTL) [15]. MTL allows one to formally express complex reactive specifications, beyond stability, trajectory tracking and the like. See examples (1) and (2).

Formally, let AP be a set of atomic propositions, which can be thought of as point-wise constraints on the state of the system. An MTL formula φ is built recursively from the atomic propositions using the following grammar:

$$\varphi := \top | p | \neg\varphi | \varphi_1 \vee \varphi_2 | \varphi_1 \wedge \varphi_2 | \varphi_1 \mathcal{U}_I \varphi_2$$

where $I \subset \mathbb{R}$ is a time interval. Here, $\top$ is the Boolean True, p is an atomic proposition, $\neg$ is Boolean negation, $\vee$ and $\wedge$ are the Boolean OR and AND operators, respectively, and $\mathcal{U}$ is the Until temporal operator. Informally, $\varphi_1 \mathcal{U}_I \varphi_2$ means that φ_1 must hold *until* φ_2 holds, and that the hand-over from φ_1 to φ_2 must happen sometime during the interval I. The implication ($\Longrightarrow$), Always ($\Box$) and Eventually ($\Diamond$) operators can be derived using the above operators.

Formally, the *semantics* of an MTL formula define what it means for a system trajectory $\mathbf{x}$ to satisfy the formula φ. Let $\mathcal{O} : AP \to \mathcal{P}(X)$ be an *observation* map for the atomic propositions. The validity (boolean truth value) of a formula φ w.r.t. the trajectory $\mathbf{x}$ at time t is defined recursively.

Definition 2.1 (MTL semantics).

$$\begin{aligned}
(\mathbf{x},t) &\models \top &&\Leftrightarrow \quad \top \\
\forall p \in AP,\ (\mathbf{x},t) &\models_{\mathcal{O}} p &&\Leftrightarrow \quad x_t \in \mathcal{O}(p) \\
(\mathbf{x},t) &\models_{\mathcal{O}} \neg\varphi &&\Leftrightarrow \quad \neg(\mathbf{x},t) \models_{\mathcal{O}} \varphi \\
(\mathbf{x},t) &\models_{\mathcal{O}} \varphi_1 \vee \varphi_2 &&\Leftrightarrow \quad (\mathbf{x},t) \models_{\mathcal{O}} \varphi_1 \vee (\mathbf{x},t) \models_{\mathcal{O}} \varphi_2 \\
(\mathbf{x},t) &\models_{\mathcal{O}} \varphi_1 \wedge \varphi_2 &&\Leftrightarrow \quad (\mathbf{x},t) \models_{\mathcal{O}} \varphi_1 \wedge (\mathbf{x},t) \models_{\mathcal{O}} \varphi_2 \\
(\mathbf{x},t) &\models_{\mathcal{O}} \varphi_1 \mathcal{U}_I \varphi_2 &&\Leftrightarrow \quad \exists t' \in t + I . (\mathbf{x},t') \models_{\mathcal{O}} \varphi_2 \\
& && \quad \wedge \forall t'' \in (t,t'),\ (\mathbf{x},t'') \models_{\mathcal{O}} \varphi_1
\end{aligned}$$

As $\mathcal{O}$ is fixed in this paper, we just drop it from the notation. We say $\mathbf{x}$ satisfies φ if $(\mathbf{x},0) \models \varphi$. All formulas that appear in this paper have bounded temporal intervals: $0 \leq \inf I < \sup I < +\infty$. To evaluate whether such a formula φ holds on a given trajectory, only a finite-length prefix of that trajectory is needed. Its length can be upper-bounded by the *horizon* of φ, $hrz(\varphi)$. The horizon is the maximum sum of all right endpoints of intervals appearing in φ [7]. Thus, we need only consider trajectories and input sequences of finite length.

2.2 Robust semantics of MTL

Designing a controller that satisfies the MTL formula φ[1] is not always enough. In a dynamic environment, where the system must react to new unforeseen events, it is useful to have a margin of maneuverability. That is, it is useful to control the system such that we *maximize* our degree of satisfaction of the formula. When unforeseen events occur, the system can react to them without violating the formula. This degree of satisfaction can be formally defined and computed using the robust semantics of MTL. Given a point $x \in X$ and a set $A \subset X$, $d_A(x) := \inf_{a \in \overline{A}} |x - a|_2$ is the distance from x to the closure $\overline{A}$ of A.

Definition 2.2 (Robustness[10]). *The* robustness *of φ relative to $\mathbf{x}$ at time t is recursively defined as*

$$\begin{aligned}
\rho_{\top}(\mathbf{x},t) &= +\infty \\
\forall p \in AP,\ \rho_p(\mathbf{x},t) &= \begin{cases} d_{X \setminus \mathcal{O}(p)}(x_t), & \text{if } x_t \in \mathcal{O}(p) \\ -d_{\mathcal{O}(p)}(x_t), & \text{if } x_t \notin \mathcal{O}(p) \end{cases} \\
\rho_{\neg\varphi}(\mathbf{x},t) &= -\rho_{\varphi}(\mathbf{x}) \\
\rho_{\varphi_1 \vee \varphi_2}(\mathbf{x},t) &= \rho_{\varphi_1}(\mathbf{x}) \sqcup \rho_{\varphi_2}(\mathbf{x}) \\
\rho_{\varphi_1 \wedge \varphi_2}(\mathbf{x},t) &= \rho_{\varphi_1}(\mathbf{x}) \sqcap \rho_{\varphi_2}(\mathbf{x}) \\
\rho_{\varphi_1 \mathcal{U}_I \varphi_2}(\mathbf{x},t) &= \sqcup_{t' \in t + \mathbb{T} I} \Big(\rho_{\varphi_2}(\mathbf{x},t') \bigsqcap \\
& \qquad \sqcap_{t'' \in [t,t')} \rho_{\varphi_1}(\mathbf{x},t'') \Big)
\end{aligned}$$

When $t = 0$, we write $\rho_{\varphi}(\mathbf{x})$ instead of $\rho_{\varphi}(\mathbf{x},0)$.

The robustness is a real-valued function of $\mathbf{x}$ with the following important property.

Theorem 2.1. *[10] For any $\mathbf{x} \in X^{\mathbb{T}}$ and MTL formula φ, if $\rho_{\varphi}(\mathbf{x},t) < 0$ then $\mathbf{x}$ falsifies the spec φ at time t, and if $\rho_{\varphi}(\mathbf{x}) > 0$ then $\mathbf{x}$ satisfies φ at t. The case $\rho_{\varphi}(\mathbf{x},t) = 0$ is inconclusive.*

Thus, we can compute control inputs by maximizing the robustness over the set of finite input sequences of a certain length. The obtained sequence $\mathbf{u}^*$ is valid if $\rho_{\varphi}(\mathbf{x},t)$ is positive, where $\mathbf{x}$ and $\mathbf{u}^*$ obey (3). The larger the magnitude $|\rho_{\varphi}(\mathbf{x},t)|$, the more robust is the behavior of the system: intuitively, $\mathbf{x}$ can be disturbed and ρ_{φ} might decrease but not go negative.

3. SMOOTH APPROXIMATION

In this section, we come up with an infinitely differentiable approximation for robustness and obtain bounds on the approximation error. We start by stating the problem we want to solve, and why the smooth approximation is helpful.

3.1 The need for smoothing

Let φ be an MTL formula with horizon N. We aim to solve the following control problem P_{ρ}.

$$P_{\rho} : \max \rho_{\varphi}(\mathbf{x}) - \gamma \sum_{k=0}^{N-1} l(x_{k+1}, u_k) \tag{4a}$$

$$\text{s.t. } x_{k+1} = f(x_k, u_k),\ \forall k = 0, \ldots, N-1 \tag{4b}$$

$$x_k \in X,\ \forall k = 0, \ldots, N \tag{4c}$$

$$u_k \in U,\ \forall k = 0, \ldots, N-1 \tag{4d}$$

$$\delta\rho_{\varphi}(\mathbf{x}) \geq 0 \tag{4e}$$

We want to use established, powerful gradient descent algorithms [21], rather than heuristics like Simulated Annealing [14]. In the above formulation, $l(x_{k+1}, u_k)$ is a system specific control cost, e.g. the LQR cost $x_k' Q x_k + u_k' R u_k$. $\gamma \geq 0$ is weighting parameter, which is a design choice. X and U define constraints on the state x and control u respectively. f represents the dynamical system, with x as the state and u as inputs. Finally, the last constraint enforces $\rho \geq 0$, i.e. the specification is satisfied. δ here is a binary design choice, 1 if the constraint is meant to be enforced, 0 otherwise. We will need to assume that f is twice

[1]Strictly speaking, a controller such that the closed-loop satisfies the formula.

Lipschitz continuously differentiable and that its gradient f_u has maximum row rank.

Gradient descent algorithms typically offer convergence guarantees to the function's minima and offer advantages which were reviewed in Sec. 1.

To apply gradient descent methods, we require a differentiable objective function. Our objective function, ρ_φ, is non-differentiable, because it uses the distance, max, and min functions, all of which are non-differentiable. One may note that these functions are all differentiable almost everywhere (a.e.). That is, the set of points in their domain where they are non-differentiable has measure 0 in $\mathbb{R}^n$. Therefore, by measure additivity, the composite function ρ_φ is itself differentiable almost everywhere. Thus, one may be tempted to 'ignore' the singularities (points of non-differentiability), and apply gradient descent to ρ_φ anyway. The rationale for doing so is that sets of measure 0 are unlikely to be visited by gradient descent, and thus don't matter. However, as we show in the next example, the lines of singularity (along which the objective is non-differentiable) can be precisely the lines along which the objective increases the fastest. See also [5]. Thus they are consistently visited by gradient descent, after which it fails to converge because of the lack of a gradient.

EXAMPLE 2. *A simple example illustrates how gradient descent gets stuck at singularities. We use the optimization algorithm Sequential Quadratic Programming (SQP) [21] to maximize the robustness of* $\varphi = \neg(x \in U)$, *where* $U = [-1,1]^2$ *is the unsafe red square in Fig. 2. In this case,* ρ_φ *is simply* $\mathbf{dist}(x_0, U)$, *the distance of the first trajectory point to the set. The search space is* $[-2.5, 2.5]^2$ *(big grey square in Fig. 2). The most robust point is* $x^* = [2.5, 2.5]$ *(green '+' in figure), being furthest from the unsafe set. We initialize the SQP at* $x_0 = [0,0]$. *SQP generates iterates (blue circles) on the line of singularity connecting* $[1,1]$ *to* x^* *and ultimately gets stuck at* $x = [1,1]$. *That's because along the line, the gradient does not exist and attempts by SQP to approximate it numerically fail, prompting it to generate smaller and smaller step-sizes for the approximation. Ultimately, SQP aborts due to the step-size being too small, and concludes it is at a local minimum.*

3.2 Approximating the distance function

To create a smooth approximation to ρ_φ, we use smooth approximations to each of its non-differentiable components: the set-distance, min, and max functions.

Recall that for a set $U \subset \mathbb{R}^n$, $\mathbf{dist}(x, U) = \inf_{a \in \overline{U}} |x - a|_2$, where $|\cdot|_2$ is the Euclidian norm. This function is globally Lipschitz with Lipschitz constant 1 and therefore differentiable almost everywhere (Rademacher's theorem), and has a second derivative almost everywhere if U is convex (Alexandrov's theorem) [17].

It is well-known that if we convolve an a.e.-differentiable function with a smooth kernel, the output function no longer has those singularities. We give an example of such a construction, which lays the groundwork for explaining the more general wavelet-based smoothing we use in the experiments. $C^\infty(\mathbb{R}^n)$ is the class of functions that are infinitely differentiable in $\mathbb{R}^n$.

THEOREM 3.1. *Consider the globally Lipschitz function* $f : \mathbb{R}^n \to \mathbb{R}$ *with Lipschitz constant* L_f. *Let* $g : \mathbb{R}^n \to \mathbb{R}_+$ *be a non-negative* $C^\infty(\mathbb{R}^n)$ *function that integrates to 1 and is supported on the unit ball:* $\int_{\mathbb{R}^n} g(x)dx = 1$, $g(x) = 0$ *if* $x \notin B(0,1)$. *Define* $g_\varepsilon = \varepsilon^{-n} g(x/\varepsilon)$ *and*

$$f_\varepsilon(x) = f * g_\varepsilon(x) = \int_{\mathbb{R}^n} f(y) g_\varepsilon(x - y) dy$$

Then f_ε *is infinitely differentiable, its Lipschitz constant* $L_{f_\varepsilon} \le L_f$ *and* $\|f - f_\varepsilon\|_\infty \le L_f \varepsilon$.

PROOF. Clearly, f_ε is C^∞: $g_\varepsilon \in C^\infty$ and the integrand in the above convolution is differentiable w.r.t. x, so it holds that $f'_\varepsilon(x) = \int f(y) \partial g_\varepsilon(x-y)/\partial x dy$.

Convolution is commutative so $f_\varepsilon(x) = \int_{\mathbb{R}^n} f(x-y) g_\varepsilon(y) dy$. Let $x' \in \mathbb{R}^n$, then

$$\begin{aligned}
|f_\varepsilon(x) - f_\varepsilon(x')| &= \left| \int_{\mathbb{R}^n} f(x-y) g_\varepsilon(y) - f(x'-y) g_\varepsilon(y) dy \right| \\
&\le \int_{\mathbb{R}^n} g_\varepsilon(y) |f(x-y) - f(x'-y)| dy \\
&= L_f |x - x'| \int_{\mathbb{R}^n} \varepsilon^{-n} g(y/\varepsilon) dy \\
&= L_f |x - x'| \int_{\mathbb{R}^n} \varepsilon^{-n} g(y') \varepsilon^n dy' \\
&= L_f |x - x'| \implies L_f \le L_{f_\varepsilon}
\end{aligned}$$

Finally,

$$\begin{aligned}
|f_\varepsilon(x) - f(x)| &= \left| \int_{\mathbb{R}^n} f(x-y) g_\varepsilon(y) dy - \int_{\mathbb{R}^n} f(x) g(y) dy \right| \\
&= \left| \int_{\mathbb{R}^n} f(x - \varepsilon y) g(y) dy - \int_{\mathbb{R}^n} f(x) g(y) dy \right| \\
&\le \int_{B(0,1)} |f(x - \varepsilon y) - f(x)| g(y) dy \\
&\le \int_{B(0,1)} L_f |\varepsilon y| g(y) dy \le L_f \varepsilon
\end{aligned}$$

In particular, $\|f - f_\varepsilon\|_\infty \to 0$ as $\varepsilon \to 0$. □

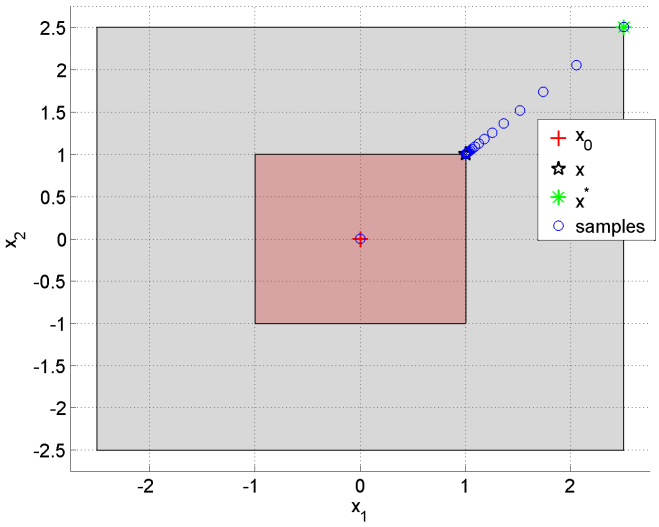
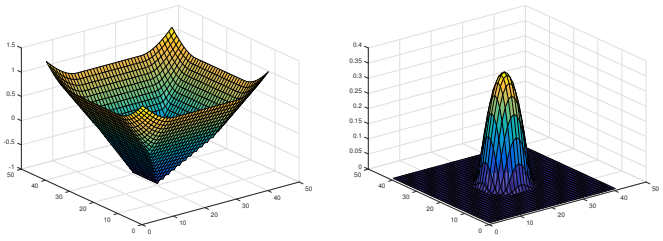


Figure 2: Iterates of SQP for Example 2. Colors in online version.

Fig. 3 shows the distance function $\mathbf{dist}(\cdot, U)$ where U is a square in the plane, smoothed by convolving with kernel g_ε obtained from the shown function. We used $\varepsilon = 0.001$, and



(a) Smoothed function (b) Function g

Figure 3: Smoothed 2-d (negative) signed distance function to a square in the x-y plane, and the function g used to smoothen it.

the actual approximation error $\|f - f_\varepsilon\|_\infty$ is less than 1e-15. Parameter ε controls how peaked or flat g_ε is: a large ε gives a peaked kernel which yields better local approximation, but the max error decreases towards 0 slower.

Wavelet approximations of the distance function. Wavelets can be viewed as a generalization of the kernel g_ε of the previous section to a whole family of kernels, obtained by translations and dilations of one function called the 'mother wavelet' ψ: $\psi_{j,k}(x) = 2^{j/2}\psi(2^j x - k)$ [18]. They are used extensively in signal processing, because their approximation properties can be tailored to the class of functions being approximated - e.g., hyperbolic wavelets are suitable for approximating functions of mixed smoothness, such as the distance function we are interested in [26].

In the experiments of this paper, we use a wavelet approximation to the distance function. Specifically, we use

$$\widetilde{\mathbf{dist}}_\varepsilon(x, U) = \sum_{(\mathbf{j},\mathbf{k})\in D} c_{\mathbf{j},\mathbf{k}}\psi_{\mathbf{j},\mathbf{k}}(x)$$

which is a partial expansion of $\mathbf{dist}(\cdot, U)$ in the wavelet basis $\{\psi_{\mathbf{j},\mathbf{k}}, \mathbf{j} = (j_1 \ldots, j_n) \in \mathbb{Z}^n, \mathbf{k} = (k_1, \ldots, k_n) \in \mathbb{Z}^n\}$. The $c_{\mathbf{j},\mathbf{k}}$ coefficients are the result of projecting $\mathbf{dist}$ onto the wavelet basis

$$c_{\mathbf{j},\mathbf{k}} = \int_{\mathbb{R}^n} \mathbf{dist}(x, U)\psi_{\mathbf{j},\mathbf{k}}dx$$

By increasing the number of terms $|D|$ in the partial expansion, we improve the accuracy of the approximation. The multi-dimensional wavelet we use is a tensor product of 1-D Meyer wavelets ψ^{meyer} [18]:

$$\psi_{\mathbf{j},\mathbf{k}} = \psi^{meyer}_{j_1,k_1} \ldots \psi^{meyer}_{j_n,k_n}, \mathbf{j}, \mathbf{k} \in \mathbb{Z}^n \quad (5)$$

3.3 Smooth max and min

We use the following standard smooth approximations of m-ary max and min. Let $k \geq 1$.

$$\widetilde{\max}_k(a_1, \ldots, a_m) := \frac{1}{k}\ln(e^{ka_1} + \ldots + e^{ka_m}) \quad (6)$$

$$\widetilde{\min}_k(a_1, \ldots, a_m) := -\widetilde{\max}(-a_1, \ldots, -a_m) \quad (7)$$

Suppose $k = 1$ and that a_1 is the largest number. Then e^{a_1} is even larger than the other e^{a_i}'s, and dominates the sum. Thus $\widetilde{\max}_1(\mathbf{a}) \approxeq \ln e^{a_1} = a_1 = \max(\mathbf{a})$. If a_1 is not significantly larger than the rest, the sum is not well-approximated by e^{a_1} alone. To counter this, the scaling factor k is used: it amplifies the differences between the numbers. It holds that for any set of m reals,

$$0 \leq \widetilde{\max}_k(a_1, \ldots, a_m) - \max(a_1, \ldots, a_m) \leq \ln(m)/k \quad (8)$$

$$0 \leq \min(a_1, \ldots, a_m) - \widetilde{\min}_k(a_1, \ldots, a_m) \leq \ln(m)/k \quad (9)$$

Indeed, the error of smooth max can be bounded as follows. Assume a_1 is the largest number, then

$$\begin{aligned}\varepsilon_M &:= \widetilde{\max}_k(\mathbf{a}) - a_1 = \frac{\ln(\sum_i e^{ka_i}) - ka_1}{k} \\ &= k^{-1}\ln\left(\frac{\sum_i e^{ka_i}}{e^{ka_1}}\right) \leq k^{-1}\ln\left(\frac{me^{ka_1}}{e^{ka_1}}\right) \\ &= \frac{\ln m}{k}\end{aligned}$$

It is also clear from what preceded that $\varepsilon_M \geq 0$. The maximum error is achieved when all the a_i's are equal.

3.4 Overall approximation

Putting the pieces together, we obtain the approximation error for the robustness of any MTL formula.

THEOREM 3.2. *Consider an MTL formula φ and reals $\varepsilon > 0$ and $k \geq 1$. Given a set U, let $\widetilde{\mathbf{dist}}_\varepsilon(\cdot, U)$ be an ε-approximation of $\mathbf{dist}(\cdot, U)$, i.e. for all x in their common domain, $|\mathbf{dist}(x, U) - \widetilde{\mathbf{dist}}_\varepsilon(x, U)| \leq \varepsilon$.*

Define the smooth robustness $\tilde{\rho}_\varphi$, obtained by substituting $\widetilde{\mathbf{dist}}_\varepsilon$ for $\mathbf{dist}$, $\widetilde{\max}_k$ for $\max$, and $\widetilde{\min}_k$ for $\min$, in Def. 2.2. Then for any length-N trajectory $\mathbf{x}$, it holds that

$$|\rho_\varphi - \tilde{\rho}_\varphi| \leq \delta_\varphi$$

where δ_φ is (a) independent of N, (b) independent of the evaluation time t, and (c) goes to 0 as $\varepsilon \to 0$ and $k \to \infty$.

PROOF. We will prove a stronger result that implies the theorem. When $\mathbf{x}$ or t are clear from the context, we will drop them from the notation.

The proof is by structural induction on φ, and works by carefully characterizing the approximation error.

Case $\varphi = p \in AP$. $\rho_\varphi(\mathbf{x}, t)$ is given by either $\mathbf{dist}x_t\mathcal{O}(p)$ or $-\mathbf{dist}x_t\mathcal{O}(p)$, and $\tilde{\rho}_\varphi(\mathbf{x}, t)$ is given by either $\widetilde{\mathbf{dist}}_\varepsilon(x_t, \mathcal{O}(p))$ or $-\widetilde{\mathbf{dist}}_\varepsilon(x_t, \mathcal{O}(p))$, respectively. Either way, $|\tilde{\rho}_\varphi(\mathbf{x}, t) - \rho_\varphi(\mathbf{x}, t)| \leq \varepsilon$. Indeed, ε satisfies the conditions on δ_φ.

Case $\varphi = \neg\varphi_1$ $|\rho_{\neg\varphi_1}(\mathbf{x}, t) - \tilde{\rho}_{\neg\varphi_1}(\mathbf{x}, t)| = |-\rho_{\varphi_1}(\mathbf{x}, t) + \rho_{\varphi_1}(\mathbf{x}, t)| \leq \delta_{\varphi_1}$, and δ_{φ_1} satisfies (a)-(c) by induction hypothesis.

Case $\varphi = \varphi_1 \vee \varphi_2$. If the same sub-formula φ_i achieves the max for both $\rho_{\varphi_1}(\mathbf{x}, t) \sqcup \rho_{\varphi_2}(\mathbf{x}, t)$ and $\tilde{\rho}_{\varphi_1}(\mathbf{x}, t) \sqcup \tilde{\rho}_{\varphi_2}(\mathbf{x}, t)$, then by induction hypothesis we immediately obtain $|\rho_\varphi(\mathbf{x}, t) - \tilde{\rho}(\mathbf{x}, t)| \leq \delta_{\varphi_i}$.

Otherwise if, say, $\rho_\varphi = \rho_{\varphi_1}$ and $\tilde{\rho}_\varphi = \tilde{\rho}_{\varphi_2}$ then

$$\rho_{\varphi_1} - \delta_{\varphi_1} \leq \tilde{\rho}_{\varphi_1} \leq \tilde{\rho}_{\varphi_2} \implies \rho_{\varphi_1} - \tilde{\rho}_{\varphi_2} \leq \delta_{\varphi_1}$$

Also

$$\tilde{\rho}_{\varphi_2} \leq \rho_{\varphi_2} + \delta_{\varphi_2} \leq \rho_{\varphi_1} + \delta_{\varphi_2} \implies -\delta_{\varphi_2} \leq \rho_{\varphi_1} - \tilde{\rho}_{\varphi_2}$$

Therefore

$$-(\delta_{\varphi_1} \sqcup \delta_{\varphi_2}) \leq \rho_{\varphi_1} - \tilde{\rho}_{\varphi_2} \leq \delta_{\varphi_1} \sqcup \delta_{\varphi_2} \Leftrightarrow |\rho_{\varphi_1} - \tilde{\rho}_{\varphi_2}| \leq \delta_{\varphi_1} \sqcup \delta_{\varphi_2}$$

Similarly, if $\rho_\varphi = \rho_{\varphi_2}$ and $\tilde{\rho}_\varphi = \tilde{\rho}_{\varphi_1}$, we have $|\rho_{\varphi_2} - \tilde{\rho}_{\varphi_1}| \leq \delta_{\varphi_1} \sqcup \delta_{\varphi_2}$. So in all cases,

$$|\rho_{\varphi_1} \sqcup \rho_{\varphi_2} - \tilde{\rho}_{\varphi_1} \sqcup \tilde{\rho}_{\varphi_2}| \leq \delta_{\varphi_1} \sqcup \delta_{\varphi_2}$$

Therefore by the triangle inequality and (8)

$$|\rho_{\varphi_1} \sqcup \rho_{\varphi_2} - \widetilde{\max}_k(\tilde{\rho}_{\varphi_1}, \tilde{\rho}_{\varphi_2})| \leq \delta_{\varphi_1} \sqcup \delta_{\varphi_2} + \ln(2)/k = \delta_\varphi$$

Clearly, δ_φ satisfied (a)-(c).

The case $\varphi_1 \wedge \varphi_2$ is treated similarly.

$\varphi = \varphi_1 \mathcal{U}_I \varphi_2$. Before proving this case, we will need the following lemma, which is provable by induction on n:

LEMMA 3.1. *If $\varphi = \varphi_1 \wedge \ldots \wedge \varphi_n$ or $\varphi = \varphi_1 \vee \ldots \vee \varphi_n$, $n \geq 2$, then $|\rho_\varphi - \tilde{\rho}_\varphi| \leq \sqcup_{1 \leq i \leq n} \delta_{\varphi_i} + \ln(n)/k$.*

We now proceed with the proof of the last case. Recall that $\rho_{\varphi_1 \mathcal{U}_I \varphi_2}(\mathbf{x}, t) = \sqcup_{t' \in t+_{\mathbb{T}} I} \left(\rho_{\varphi_2}(\mathbf{x}, t') \sqcap \right.$ $\left. \sqcap_{t'' \in [t,t')} \rho_{\varphi_1}(\mathbf{x}, t'')\right)$. Starting with the innermost sub-expression $\rho_\psi := \sqcap_{t'' \in [t,t')} \rho_{\varphi_1}(\mathbf{x}, t'')$, we have, by Lemma 3.1

$$|\rho_\psi - \tilde{\rho}_\psi| \leq \sqcup_{t'' \in [t,t')} \delta_{\varphi_1}^{t''} + \ln(t' - t)/k \qquad (10)$$

where $\delta_{\varphi_1}^{t''}$ is the bound for approximating $\rho_{\varphi_1}(\mathbf{x}, t'')$. But δ_φ does not depend on the time at which the formula is evaluated. Therefore the bound in (10) becomes

$$|\rho_\psi - \tilde{\rho}_\psi| \leq \delta_{\varphi_1} + \ln(t' - t)/k \qquad (11)$$

To avoid introducing a dependence on time, we further upper-bound by

$$|\rho_\psi - \tilde{\rho}_\psi| \leq \delta_{\varphi_1} + \ln(hrz(\varphi))/k := \delta_\psi$$

where, recall, $hrz(\varphi)$ is the horizon of φ (see Section 2.1).

Continuing with the sub-expression $\rho_\alpha = \rho_{\varphi_2}(\mathbf{x}, t') \sqcap \rho_\psi$, by the induction hypothesis it holds that $|\rho_\alpha - \tilde{\rho}_\alpha| \leq \delta_{\varphi_2} \sqcup \delta_\psi + \ln(2)/k := \delta_\alpha$. Finally, the top-most max operator introduces the total error

$$\begin{aligned} |\rho_\varphi - \tilde{\rho}_\varphi| &\leq \delta_\alpha + \ln(|I|)/k \\ &= \delta_{\varphi_2} \sqcup \delta_\psi + \ln(2)/k + \ln(|I|)/k \\ &= \delta_{\varphi_2} \sqcup (\delta_{\varphi_1} + \ln(hrz(\varphi))/k) + \ln(2|I|)/k \\ &= \delta_\varphi \qquad (12) \end{aligned}$$

The first inequality obtains from the fact that δ_α is independent of evaluation time and Lemma 3.1. The bound δ_φ obeys (a)-(c). This concludes the proof. □

REMARK 3.1. *The proof suggests in (12) that every Until operator increases the error by $+\ln(hrz(\varphi))/k$, which may be a large quantity for long-horizon formulas. However, a more careful analysis of the accumulation of interval widths $t' - t$, which we upper bounded above by $hrz(\varphi)$, reveals that that is not the case. Indeed, consider the formula*

$$\varphi = \underbrace{(\varphi_1 \mathcal{U}_{[a,b]} \varphi_2)}_{\psi} \mathcal{U}_{[c,d]} \varphi_3$$

where φ_i does not contain temporal operators and let t_ψ be the satisfaction time of ψ. I.e. it is the time in $[a, b]$ when φ_2 becomes true and 'takes over' from φ_1. Then, using (11), δ_φ is equal to

$$\begin{aligned} & \delta_{\varphi_3} \sqcup (\delta_\psi + \ln(t_{\varphi_3} - t_\psi)/k) + \ln(2[d-c])/k \\ \leq\ & \delta_{\varphi_3} \sqcup (\delta_\psi + \ln(t_\psi + d - t_\psi)/k) + \ln(2[d-c])/k \\ \leq\ & \delta_{\varphi_3} \sqcup (\delta_\psi + \ln(d)/k) + \ln(2[d-c])/k \\ =\ & \delta_{\varphi_3} \sqcup \left(\underbrace{\delta_{\varphi_2} \sqcup (\delta_{\varphi_1} + \ln(b)/k) + \ln(2[b-a])/k}_{\delta_\psi} + \ln(d)/k \right) \\ & + \ln(2[d-c])/k \end{aligned}$$

The sum of interval widths, such as $\ln(2[b-a]) + \ln(2[d-c])$ in this example, gives a total $\sum_j \ln(2|I_j|) = \#\mathcal{U} \ln(2) + \sum \ln(|I_j|)$, where $\#\mathcal{U}$ is the number of times $\mathcal{U}$ appears in φ and the I_j's are all the temporal intervals. This quantity, in most cases, will actually be smaller than the horizon. The sum of interval right endpoints, such as $\ln(b)/k + \ln(d)/k$ in this example, yields $\sum_j \ln(\sup I_j)/k$ in total, which is smaller than the horizon.

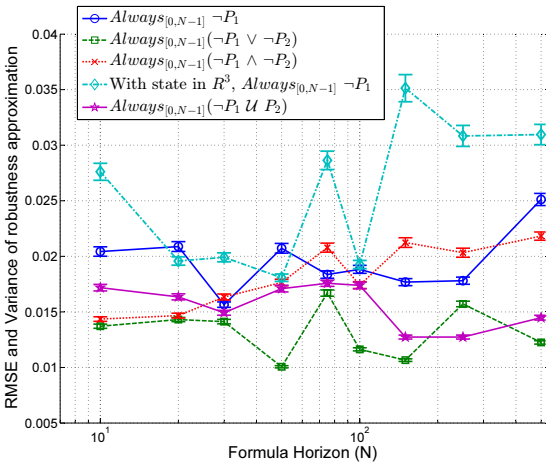


Figure 4: RMSE (and variance) of robustness approximation error against formula horizon, evaluated on 1000 randomly generated trajectories for the system in (13). Unless noted, the states in the trajectory are in $\mathbb{R}^2$. Note, the magnitude of the approximation errors are very small, as is the variance, showing the accuracy of the smooth approximation of robustness.

4. APPROXIMATION ERROR, VERIFICATION AND CONTROL

We implemented the above smooth approximation to the semantics of MTL, and tested it empirically on a number of examples.

4.1 Approximation error for robustness

We evaluated the robustness ρ_φ and its approximation $\tilde{\rho}_\varphi$ for five formulae, with $hrz(\varphi_i) = N$. P_1 and P_2 are atomic propositions for state being in two polyhedrons P_1 and P_2 respectively. Each formula's robustness is evaluated on 1000 randomly-generated trajectories of varying lengths N, so we can examine the error's variation with the horizon. The trajectories were produced by a 2-or-3 dimensional system, (13) with input and state saturation.

Fig. 4 shows the Root Mean Square (RMSE) of the approximation, $\sqrt{(1/1000)\sum_{\mathbf{x}}(\rho_\varphi(\mathbf{x}) - \tilde{\rho}_\varphi(\mathbf{x}))^2}$, and variance bars around it. As suggested by Remark 3.1, the approximation error generally increases with the horizon (for a constant number of wavelet coefficients). This is due to the smooth max and min functions, as seen in (8).

Fig. 5 shows the relative approximation errors, $(\rho_\varphi - \tilde{\rho}_\varphi)/|\rho_\varphi|$, for the formulae under consideration. It is seen that the average relative approximation error is less than 10% for all cases. For some data points in Fig. 5, the variance of relative error is high, but the error remains small in absolute terms as seen in Fig. 4.

Note that while the RMSE increased with the system dimension (4^{th} formula in Fig. 4), the relative error remained very small (4^{th} formula in Fig. 5), i.e. the increase in error is explained by an increase in the robustness's value.

4.2 Robustness maximization for control

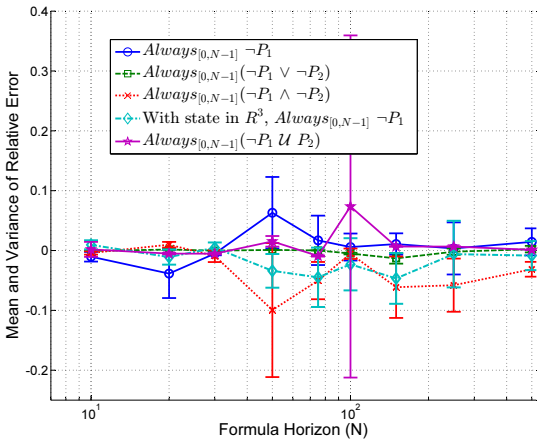


Figure 5: Mean and variance of relative approximation error against formula horizon, evaluated on 1000 randomly generated trajectories for the system in (13). Unless noted, the states in the trajectory are in $\mathbb{R}^2$.

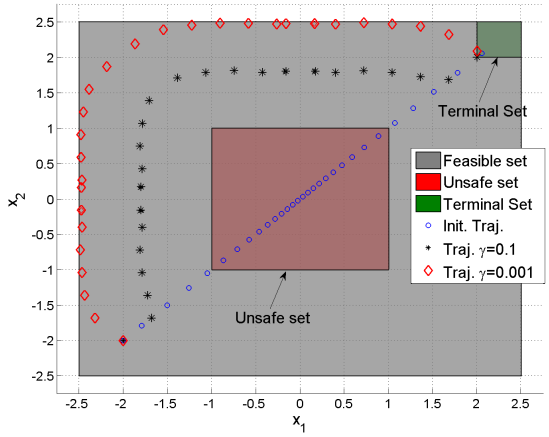


Figure 6: Initial trajectory and trajectories obtained for two different values of γ in (4).

To solve Problem P_ρ given in (4), we replace the true robustness ρ_φ by its smooth approximation $\tilde{\rho}_\varphi$. We thus obtain Problem $P_{\tilde{\rho}}$. We illustrate the approach on a simple linear system, and provide more extensive case studies in Section 5.

4.2.1 *Illustrative example*

We consider a linear system with the following dynamics:

$$x_{k+1} = x_k + u_k \tag{13}$$

The specification is

$$\varphi = \square_{[0,20]} \neg(x_k \in \text{Unsafe}) \wedge \Diamond_{[0,20]}(x_k \in \text{Terminal})$$

with the sets Unsafe $= [-1,1]^2$ i.e. a hyper-cube in $\mathbb{R}^2$ with length 2, centered on the origin) and Terminal $= [2, 2.5]^2$. The state space is $X = [-2.5, 2.5]^2$, $U = [0.3, 0.3]^2$, $\delta = 1$, and we optimize for two different values of γ, 0.1 and 0.001. The initial point of the optimization is $x_0 = [-2, -2]'$. The control cost is $l(x_k, u_k) = ||x_k||_2^2$, so that $\sum_k l(x_k, u_k)$ penalizes the length of the trajectory. Here, $hrz(\varphi) = 21$.

Optimization solver. We use Sequential Quadratic Programming (SQP) to solve the optimization problem $P_{\tilde{\rho}}$. SQP solves constrained non-linear optimization problems, like $P_{\tilde{\rho}}$, by creating a sequence of quadratic approximations to the problem and solving these approximate problems. SQP enjoys various convergence-to-(local)-minima properties, depending on the assumptions we place on the problem. See [21, Section 2.9]. For example, for SQP to converge to a strict local minimum (a minimum that is strictly smaller than any objective function value in an open neighborhood around it), it suffices that 1) all constraint functions be twice Lipschitz continuously differentiable (which is true in our case), and 2) at points in the search space that lie on the boundary of the inequality-feasible set (where the inequality constraints are satisfied with equality), there exists a search direction towards the interior of the feasible set that does not violate the equality constraints (the so-called Mangasarian-Fromowitz constraint qualification) [21, Assumption 2.9.1]. This is also true in our case since our equality constraints come from the dynamics and are always enforced for any $\mathbf{u}$.

Solver initialization. To initialize SQP (i.e., give it a starting point for the optimization), we need an *initial trajectory* that starts from x_0 and ends in the Terminal set. We obtain this initial trajectory the standard way, by solving a feasibility linear program with constraints (4b)-(4d). By definition, the solution to a feasibility program is a trajectory that simply satisfies the constraints without optimizing the objective.

Results. Fig. 6 shows the sets, initial trajectory (which is unsafe and has a robustness of -1), and the two trajectories for the two values of γ. Both trajectories satisfy the specification φ. Intuitively, the trajectories in Fig.6 make sense, as for a higher value of $\gamma = 0.1$ we get a shorter trajectory, which is closer to unsafe set, hence satisfies φ less robustly ($\rho_\varphi = 0.65$) and for a smaller value of $\gamma = 0.001$ we get a longer trajectory with a higher robustness ($\rho_\varphi = 1.21$).

5. CASE STUDIES

To evaluate our approach, we solve a robustness maximization problem for control of two systems, using three methods (all of which are implemented in MATLAB)

- SR-SQP, which uses SQP to optimize the smooth approximation to robustness, $\tilde{\rho}_\varphi$
- R-SQP, which uses SQP to optimize the *true* robustness, ρ_φ
- SA, which uses Simulated Annealing to optimize ρ_φ.

For both examples considered here, first, we compute the wavelet approximation of the distance function to the sets $\mathcal{O}(p)$ off-line. Next, we solve the control problem (4) as a single shot, finite horizon constrained optimization.

5.1 HVAC Control of a building for comfort

We evaluate the control performance of our approach (SR-SQP) and compare it to R-SQP and SA. This is done by testing it on the Heating, Ventilation and Air Conditioning (HVAC) control of a 4-state model of a single zone in a building. Such a model is commonly used in literature for evaluation of predictive control algorithms [13]. The control problem we solve is similar to the example used in [22], where the objective is to bring the zone temperature to a

comfortable range when the zone is occupied (given predictions on the building occupancy). The specification is:

$$\varphi = \Box_I(\text{ZoneTemp} \in \text{Comfort}) \tag{14}$$

Here, I is the time interval where the zone is occupied, and Comfort is the range of temperatures (in Celsius) deemed comfortable ($[22, 28]$). For the control horizon, we consider a 24 hour period, in which the building is occupied from time steps 10 to 19 (i.e. $I = [10, 19]$), i.e. a 10-hour workday.

System dynamics. The single-zone model, discretized at a sampling rate of 1 hour (which is common in building temperature control) is of the form:

$$x_{k+1} = Ax_k + Bu_k + B_d d_k \tag{15}$$

Here, A, B and B_d matrices are from the hamlab ISE model [25]. $x \in \mathbb{R}^4$ is the state of the model, the 4^{th} element of which is the zone temperature, the others are auxiliary temperatures corresponding to other physical properties of the zone (walls and facade). The input to the system, $u \in \mathbb{R}^1$, is the heating/cooling energy. $b_d \in \mathbb{R}^3$ are disturbances (due to occupancy, outside temperature, solar radiation). We assume these are known a priori. The control problem we solve is of the form in (4), with γ and δ both set to zero, and $X = [0, 50]^4$, $U = [-1000, 2000]$.

Results. To initialize the optimization for all three methods, we generate an initial trajectory for the system (15), starting from $x_0 = [21, 21, 21, 21]'$, which does not satisfy φ. The final trajectories after optimization from the three methods are shown in Fig.7. Our method (SR-SQP) and SA both result in trajectories that satisfy φ, with a robustness of 2.9994 and 2.8862 respectively. On the other hand, R-SQP results in a trajectory that does not satisfy φ ($\rho_\varphi = -0.1492$), and terminates on a local maxima.

Analysis. In this particular problem, the maximum robustness achievable is 3, which can be achieved by setting the room temperature at 25C for the interval I. With this insight, the problem of maximizing robustness can be solved with a quadratic program with linear constraints and the cost $\sum_{k\in I}(x_{4k} - 25)^2$ to be minimized. This indeed results in a trajectory with the global optimal robustness of 3, but this is a method tailored to the particular problem.

SR-SQP, which is a general purpose technique, results in a robustness which is just 0.02% less than the global optimal value. In the following example, we take a specification which cannot be trivially turned into a quadratic-program.

5.2 Autonomous ATC for quad-rotors

Air Traffic Control (ATC) offers many opportunities for automation to allow safer and more efficient landing patterns. The constraints of ATC are complex and contain many safety rules [16]. In this example we formalize a subset of such rules, similar to those in example 1, for an autonomous ATC for quad-rotors in MTL. We demonstrate how the smoothed robustness is used to generate control strategies for safely and robustly landing two quad-rotors in an enclosed airspace with an obstacle.

The specification. The specification for the autonomous

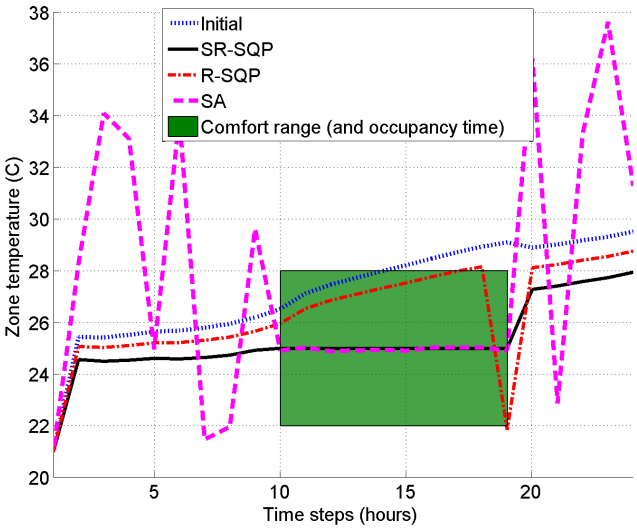


Figure 7: Zone temperatures. The green rectangle shows the comfortable temperature limit of 22-28 C, applicable during time steps 10-19 (when the building is occupied).

ATC with two quad-rotors is:

$$\begin{aligned}
\varphi = {} & \Diamond_{[0,N-1]}(q_1 \in \text{Terminal}) \wedge \Diamond_{[0,N-1]}(q_2 \in \text{Terminal}) \wedge \\
& \Box_{[0,N-1]}(q_1 \in \text{Zone}_1 \implies z_1 \in [1, 5]) \wedge \\
& \Box_{[0,N-1]}(q_2 \in \text{Zone}_1 \implies z_2 \in [1, 5]) \wedge \\
& \Box_{[0,N-1]}(q_1 \in \text{Zone}_2 \implies z_1 \in [0, 3]) \wedge \\
& \Box_{[0,N-1]}(q_2 \in \text{Zone}_2 \implies z_2 \in [0, 3]) \wedge \\
& \Box_{[0,N-1]}(\neg(q_1 \in \text{Unsafe})) \wedge \Box_{[0,N-1]}(\neg(q_2 \in \text{Unsafe})) \wedge \\
& \Box_{[0,N-1]}(||q_1 - q_2||_2^2 \geq d_{min}^2)
\end{aligned} \tag{16a}$$

Here q_1 and q_2 refer to the position of the two quad-rotors in (x, y, z)-space, and z_1 and z_2 refer to their altitude. The specification says that, within a horizon of N steps, both quad-rotors should: a) Eventually land (reach the terminal zone), b) Follow altitude rules in two zones, Zone_1 and Zone_2 which have different altitude floors and ceilings, c) Avoid the Unsafe set, and d) always maintain a safe distance between each other (d_{min}).

Note that turning the specification into constraints for the control problem is no longer simple. This is due to the $\Diamond$ operator, which would require a MILP formulation to be accounted for. In addition, the minimum separation and altitude rules for the two zones cannot be turned into convex constraints for the optimization. As will be seen below, our approach allows us to keep the non-convexity in the cost function, and have convex (linear) constraints on the optimization problem.

System dynamics. The airspace and associated sets for the specification φ are hyper-rectangles in $\mathbb{R}^3$ (visualized in Fig. 8), except the altitude floor and ceiling limit, which is in $\mathbb{R}^1$. In simulation, d_{min} is set to 0.2 m.

The quad-rotor dynamics are obtained via linearization around hover, and discretization at 5-Hz. Similar models have been used for control of real quad-rotors with success ([20]). For simulation, we set the mass of either quad-rotor to be 0.5 kg. The corresponding linearized and discretized quad-rotor dynamics are given as:

$$\begin{bmatrix} \dot{x}_{k+1} \\ \dot{y}_{k+1} \\ \dot{z}_{k+1} \\ x_{k+1} \\ y_{k+1} \\ z_{k+1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0.2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0.2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0.2 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \dot{x}_k \\ \dot{y}_k \\ \dot{z}_k \\ x_k \\ y_k \\ z_k \end{bmatrix} + \begin{bmatrix} 1.96 & 0 & 0 \\ 0 & -1.96 & 0 \\ 0 & 0 & 0.4 \\ 0.196 & 0 & 0 \\ 0 & -0.196 & 0 \\ 0 & 0 & 0.04 \end{bmatrix} \begin{bmatrix} \theta_k \\ \phi_k \\ \mathrm{T}_k \end{bmatrix} \tag{17}$$

Here, the state consists of the velocities and positions in the x, y, z co-ordinates. The inputs to the system are the desired roll angle θ, pitch angle ϕ and thrust T.

The control problem. For the autonomous ATC problem for two quad-rotors, we solve (4) with $\tilde{\rho}$ in the objective instead of ρ. Note, we set $\gamma = 0$ here, following logically from existing ATC rules (see sec.1), which do not have an air-craft specific cost for fuel, or distance traveled. Because of this, we can also set $\delta = 0$ and simply maximize(smooth) robustness (subject to system dynamics and constraints) to get trajectories that satisfy φ. For the control problem, X and U represent the bounds on the states (Airspace and velocity limits) and inputs respectively, for both quad-rotors. f represents the linearized dynamics of (17) applied to two quad-rotors, and $N = 21$. The initial state for the first quad-rotor is $[2, 2, 2, 0, 0, 0]'$ and for the second, $[2, -2, 2, 0, 0, 0]'$.

Results. For each approach, we ran three optimizations, starting from three different trajectories to initialize the optimization. These *initial trajectories* can be obtained in practice by a fast trajectory generator. The three initial trajectories all have negative robustness, i.e. they violate φ.

Fig.8 shows the three trajectories obtained after applying SR-SQP, with the three initial trajectories as initial guesses for the optimizations. All three trajectories obtained by SR-SQP satisfy the specification φ. To avoid visual clutter, we do not show the trajectories obtained from the other two methods on the figure. Instead, we summarize the results in Table 1 which shows the true robustness of the three initial trajectories, and the true robustness for the trajectories obtained via the three methods, SR-SQP, SA, and R-SQP.In order to keep the study easy to interpret, we use two quad-rotors, but it is straight forward to scale the specification and the optimization to account for more.

Analysis. It is seen that SR-SQP and R-SQP satisfy φ for all instances, while SA satisfies it only once. Note that in all three cases, R-SQP results in trajectories with the same robustness value. We conjecture that this is because R-SQP is getting stuck at local minima at points of non-differentiability of the objective, as illustrated in Example 2. On further investigation, we also noticed that the robustness value achieved is due to the segment of the φ corresponding to $\diamondsuit_{[0,N]}(q_2 \in \text{Terminal})$. R-SQP does not drive the trajectory (for quad-rotor 2) deeper inside the set Terminal, unlike the proposed approach, SR-SQP, even though the minimum separation property is far from being violated. This lends credence to our hypothesis of SQP terminating on a local minima, which is the flag MATLAB's optimization gives.

Table 1: Robustness of final trajectory $\mathbf{x}^*$ for three optimization runs with different initial trajectories.

Run	$\rho(\mathbf{x}_0)$	SR-SQP $\rho(\mathbf{x}^*)/\tilde{\rho}$	SA: $\rho(\mathbf{x}^*)$	R-SQP: $\rho(\mathbf{x}^*)$
1	-0.8803	**0.2985** / 0.2460	-0.2424	0.1798
2	-0.7832	**0.3255** / 0.3103	-0.5861	0.1798
3	-0.0399	**0.2967** / 0.2652	0.0854	0.1798

5.3 Discussion

With two case studies on dynamic systems, we show the applicability and consistently good performance of our method, SR-SQP, which outperforms both SA and R-SQP. For every instance we covered, SR-SQP finds trajectories that satisfy the specification, while the other two methods do not always do so.

While we solve the control problem in a single-shot, finite horizon manner, in general, for a real-time implementation, the problem can be solved in a receding horizon manner (similar to [20], [13]). Or, it can be solved in a manner where the state and actions of the past are stored an added as constraints at each time step while the look-ahead horizon of the optimization shrinks (similar to [22]). This will be explored further in future work. We have shown previously [20] that control of an actual quad-rotor with the dynamics in (17) is possible on a low computation power platform. The control algorithm there involved solving multiple quadratic programs at even higher sampling rates ($20Hz$), in a receding horizon manner. Future work will include a C implementation of SR-SQP, which will allow us to experiment on real platforms, like the aforementioned quad-rotors.

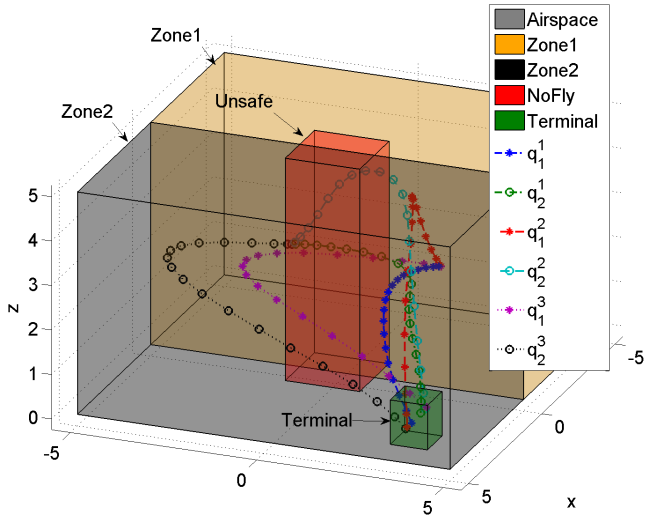


Figure 8: Trajectories obtained via SQP on smooth robustness, with three different initial trajectories acting as initial solutions for the SQP. Note, all 3 trajectories satisfy φ. Here, q_i^j refers to the positions of the i^{th} initial trajectory for the j^{th} quadrotor. Consider q_1^1 and q_2^1, the first trajectory for the two quad-rotors. The second quad-rotor swerves around the obstacle and reaches Terminal, while the first quad-rotor swerves towards Unsafe, without violating φ, in order to maintain a safe distance with the other quad-rotor while reaching Terminal. This results in the two quad-rotors satisfying φ. Similar behavior is seen with the other two trajectories as well. A real-time playback of trajectories can be seen in http://bit.ly/2dY4xjw.

6. CONCLUSIONS

We present a method to obtain smooth (infinity differentiable) approximations to the robustness of MTL formulae, with bounded and asymptotically decaying approximation error. Empirically, we show that the approximation error is indeed small for a variety of commonly used MTL formulae. Through several examples, we show how we leverage the smoothness property of the approximation for solving a control problem by maximizing the smooth robustness, using SQP, an off-the-shelf gradient descent optimization

technique. A similar approach can also be used for falsification by minimizing the smooth robustness over a set of possible initial states for a closed loop system. We compare our technique (SR-SQP) to two other approaches for robustness maximization for control of two dynamical systems, with state and input constraints, and show how our approach consistently outperforms the other two and can be used for control of systems to satisfy MTL specifications.

7. REFERENCES

[1] H. Abbas and G. Fainekos. Linear hybrid system falsification through local search. In *Automated Technology for Verification and Analysis*, volume 6996 of *LNCS*, pages 503–510. Springer, 2011.

[2] H. Abbas and G. Fainekos. Convergence proofs for simulated annealing falsification of safety properties. In *Proc. of 50th Annual Allerton Conference on Communication, Control, and Computing*. IEEE Press, 2012.

[3] H. Abbas and G. Fainekos. Computing descent direction of MTL robustness for non-linear systems. In *American Control Conference*, 2013.

[4] H. Abbas, A. Winn, G. Fainekos, and A. A. Julius. Functional gradient descent method for metric temporal logic specifications. In *2014 American Control Conference*, pages 2312–2317, June 2014.

[5] J. Cortes. Discontinuous dynamical systems. *IEEE Control Systems*, 28(3):36–73, June 2008.

[6] J. Deshmukh, G. Fainekos, J. Kapinski, S. Sankaranarayanan, A. Zutshi, and Xiaoqing Jin. Beyond single shooting: Iterative approaches to falsification. In *2015 American Control Conference (ACC)*, pages 4098–4098, July 2015.

[7] A. Dokhanchi, B. Hoxha, and G. Fainekos. Online monitoring for temporal logic robustness. In *Proceedings of Runtime Verification*, 2014.

[8] A. Donzé and O. Maler. *Robust Satisfaction of Temporal Logic over Real-Valued Signals*, pages 92–106. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[9] T. Dreossi, T. Dang, A. Donze, J. Kapinski, X. Jin, and J. V. Deshmukh. A trajectory splicing approach to concretizing counterexamples for hybrid systems. In *NASA Symposium on Formal Methods*, 2015.

[10] G. Fainekos and G. Pappas. Robustness of temporal logic specifications for continuous-time signals. *Theoretical Computer Science*, 410(42):4262–4291, September 2009.

[11] G. E. Fainekos, S. Sankaranarayanan, K. Ueda, and H. Yazarel. Verification of automotive control applications using s-taliro. In *2012 American Control Conference (ACC)*, pages 3567–3572, June 2012.

[12] G.E. Fainekos, A. Girard, and G. Pappas. *Temporal Logic Verification Using Simulation*, pages 171–186. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.

[13] A. Jain, M. Behl, and R. Mangharam. Data predictive control for building energy management (submitted to the acc). 2017.

[14] S. Kirkpatrick, D. Gelatt Jr., and M.P. Vecchi. Optimization by simulated annealing. *Science*, 220(4598):671–680, 1983.

[15] R. Koymans. Specifying real-time properties with metric temporal logic. *Real-Time Systems*, 2(4):255–299, 1990.

[16] M. Z. Li and M. S. Ryerson. Modeling and estimating airspace movements using air traffic control transcription data, a data-driven approach. In *International Conference on Research in Air Transportation*, 2016.

[17] M. M. Makela and P. Neittaanmaki. *Nonsmooth optimization*. World Scientific, 1992.

[18] S. G. Mallat. *A Wavelet Tour of Signal Processing, Third Edition: The Sparse Way*. Academic Press, 2008.

[19] T. Nghiem, S. Sankaranarayanan, G. Fainekos, F. Ivancic, A. Gupta, and G. Pappas. Monte-carlo techniques for falsification of temporal properties of non-linear hybrid systems. In *Hybrid Systems: Computation and Control*, 2010.

[20] Y. V. Pant, K. Mohta, H. Abbas, T. X. Nghiem, J. Devietti, and R. Mangharam. Co-design of anytime computation and robust control. In *RTSS*, pages 43–52, Dec 2015.

[21] E. Polak. *Optimization: Algorithms and Consistent Approximations*. Springer-Verlag New York, Inc., New York, NY, USA, 1997.

[22] V. Raman, A. Donze, M. Maasoumy, R. M. Murray, A. Sangiovanni-Vincentelli, and S. A. Seshia. Model predictive control with signal temporal logic specifications. In *53rd IEEE Conference on Decision and Control*, pages 81–87, Dec 2014.

[23] S. Sankaranarayanan and G. Fainekos. Falsification of temporal properties of hybrid systems using the cross-entropy method. In *ACM International Conference on Hybrid Systems: Computation and Control*, 2012.

[24] S. Sankaranarayanan and G. Fainekos. Simulating insulin infusion pump risks by in-silico modeling of the insulin-glucose regulatory system. In *International Conference on Computational Methods in Systems Biology*, 2012.

[25] A Van Schijndel. Integrated heat, air and moisture modeling and simulation in hamlab. In *IEA Annex 41 working meeting, Montreal, May*, 2005.

[26] H. Wang. Representation and approximation of multivariate functions with mixed smoothness by hyperbolic wavelets. *Journal of Mathematical Analysis and Applications*, 291(2):698 – 715, 2004.