Composing Control Barrier Functions for Complex Safety Specifications

Tamas G. Molnar and Aaron D. Ames

Abstract— **The increasing complexity of control systems necessitates control laws that guarantee safety w.r.t. complex combinations of constraints. In this letter, we propose a framework to describe compositional safety specifications with control barrier functions (CBFs). The specifications are formulated as Boolean compositions of state constraints, and we propose an algorithmic way to create a single continuously differentiable CBF that captures these constraints and enables safety-critical control. We describe the properties of the proposed CBF, and we demonstrate its efficacy by numerical simulations.**

I. INTRODUCTION

Control designs with formal safety guarantees have long been of interest in engineering. Safety is often captured as constraints on the system's states that must be enforced for all time by the controller. To enable the satisfaction of state constraints with formal guarantees of safety, control barrier functions (CBFs) [1] have become a popular tool in nonlinear control design. As the complexity of safety-critical control systems increases, complex combinations of multiple safety constraints tend to arise, which creates a need for controllers incorporating multiple CBFs.

The literature contains an abundance of studies on multiple safety constraints. Some approaches directly used multiple CBFs in control design. For example, [2], [3] directly imposed multiple CBF constraints on the control input in optimization-based controllers; [4] synthesized controllers by switching between multiple CBFs whose superlevel set boundaries do not intersect; [5] investigated the compatibility of CBFs; [6] ensured feasible controllers with multiple CBFs; and [7], [8] addressed multi-objective constraints via barrier Lyapunov functions. These works usually linked safety constraints with AND logic: they maintained safety w.r.t. constraint 1 AND constraint 2, etc. Other approaches combined multiple constraints into a single CBF. These include versatile combinations, such as Boolean logic with both AND, OR and negation operations, which was established in [9], [10] by nonsmooth barrier functions. Similarly, [11] used Boolean logic to create a smooth CBF restricted to a safe set in the state space; [12] combined CBFs with AND logic via parameter adaptation; while [13], [14] used signal temporal logic to combine CBFs in a smooth manner.

In this letter, we propose a framework to capture complex safety specifications by CBFs. We combine multiple safety constraints via Boolean logic, and propose an algorithmic way to establish a single CBF for nontrivial safety specifications. Our method leverages both the Boolean logic from [9] and the smooth combination idea from [13], while merging the benefits of these approaches. We address multiple levels of logical compositions of safety constraints, i.e., arbitrary combinations of AND and OR logic, which was not established in [13], while we create a continuously differentiable CBF to avoid discontinuous systems like in [9]. Meanwhile, as opposed to [11], the stability of the safe set is guaranteed.

In Section II, we introduce CBFs and motivate multiple safety constraints. In Section III, we propose a single CBF candidate to address the compositions of multiple constraints. We also characterize its properties, and we use simulations to demonstrate its ability to address safety-critical control with nontrivial constraints. Section IV closes with conclusions.

II. CONTROL BARRIER FUNCTIONS

We consider affine control systems with state $x \in \mathbb{R}^n$, control input $u \in \mathbb{R}^m$, and dynamics:

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

where $f : \mathbb{R}^n \to \mathbb{R}^n$ and $g : \mathbb{R}^n \to \mathbb{R}^{n \times m}$ are locally Lipschitz. Our goal is to design a controller $k : \mathbb{R}^n \to \mathbb{R}^m$, $u = k(x)$ such that the closed-loop system:

$$\dot{x} = f(x) + g(x)k(x), \tag{2}$$

satisfies certain safety specifications.

If k is locally Lipschitz, then for any initial condition $x(0) = x_0 \in \mathbb{R}^n$ system (2) has a unique solution $x(t)$, which we assume to exist for all $t \geq 0$. We say that the system is safe if the solution $x(t)$ evolves inside a *safe set* $\mathcal{C}$. Specifically, we call (2) *safe w.r.t.* $\mathcal{C}$ if $x_0 \in \mathcal{C} \implies x(t) \in \mathcal{C}$ $\forall t \geq 0$. We define the safe set as the 0-superlevel set of a continuously differentiable function $h : \mathbb{R}^n \to \mathbb{R}$:

$$\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}, \tag{3}$$

assuming it is non-empty and has no isolated points. Later we extend this definition to more complex safety specifications.

The input u affects safety through the derivative of h:

$$\dot{h}(x, u) = \underbrace{\nabla h(x) f(x)}_{L_f h(x)} + \underbrace{\nabla h(x) g(x)}_{L_g h(x)} u, \tag{4}$$

where $L_f h$ and $L_g h$ are the Lie derivatives of h along f and g. By leveraging this relationship, *control barrier functions (CBFs)* [1] provide controllers with formal safety guarantees.

Definition 1 ([1]). Function h is a *control barrier function* for (1) on $\mathbb{R}^n$ if there exists $\alpha \in \mathcal{K}^{\rm e}_\infty$[1] such that for all $x \in \mathbb{R}^n$:

$$\sup_{u \in \mathbb{R}^m} \dot{h}(x, u) \geq -\alpha\big(h(x)\big). \tag{5}$$

*This research is supported in part by the National Science Foundation (CPS Award #1932091) and Nodein Inc.

T. G. Molnar and A. D. Ames are with the Department of Mechanical and Civil Engineering, California Institute of Technology, Pasadena, CA 91125, USA, tmolnar@caltech.edu, ames@caltech.edu.

[1] Function $\alpha : (-b, a) \to \mathbb{R}$, $a, b > 0$ is of extended class-$\mathcal{K}$ ($\alpha \in \mathcal{K}^{\rm e}$) if it is continuous, strictly increasing and $\alpha(0) = 0$. Function $\alpha : \mathbb{R} \to \mathbb{R}$ is of extended class-$\mathcal{K}_\infty$ ($\alpha \in \mathcal{K}^{\rm e}_\infty$) if $\alpha \in \mathcal{K}^{\rm e}$ and $\lim_{r \to \pm\infty} \alpha(r) = \pm\infty$.

Note that the left-hand side of (5) is $L_f h(x)$ if $L_g h(x) = 0$ and it is ∞ otherwise. Thus, (5) is equivalent to[2]:

$$L_g h(x) = 0 \implies L_f h(x) + \alpha\big(h(x)\big) \geq 0. \tag{6}$$

Given a CBF, [1] established safety-critical control.

Theorem 1 ([1], [16])**.** *If h is a CBF for* (1) *on $\mathbb{R}^n$, then any locally Lipschitz controller k that satisfies:*

$$\dot{h}\big(x, k(x)\big) \geq -\alpha\big(h(x)\big) \tag{7}$$

for all $x \in \mathcal{C}$ renders (2) *safe w.r.t. $\mathcal{C}$. Furthermore, if* (7) *holds for all $x \in \mathbb{R}^n$, then $\mathcal{C}$ is asymptotically stable.*

Accordingly, if the controller k is synthesized such that (7) holds for all $x \in \mathcal{C}$, then the closed-loop system evolves in the safe set: $x_0 \in \mathcal{C} \implies x(t) \in \mathcal{C}\ \forall t \geq 0$. Moreover, even if the initial condition is outside $\mathcal{C}$, i.e., $x_0 \notin \mathcal{C}$, the system converges towards $\mathcal{C}$ if (7) is enforced for all $x \in \mathbb{R}^n$ [16].

Condition (7) is often used as constraint in optimization to synthesize safe controllers. For example, a desired but not necessarily safe controller $k_{\rm d} : \mathbb{R}^n \to \mathbb{R}^m$ can be modified to a safe controller via the *quadratic program (QP)*:

$$\begin{aligned} k(x) = \underset{u \in \mathbb{R}^m}{\operatorname{argmin}} \quad & \|u - k_{\rm d}(x)\|^2 \\ \text{s.t.} \quad & \dot{h}(x, u) \geq -\alpha\big(h(x)\big), \end{aligned} \tag{8}$$

also known as *safety filter*, which has explicit solution [17]:

$$k(x) = \begin{cases} k_{\rm d}(x) + \max\{0, \eta(x)\} \frac{L_g h(x)^\top}{\|L_g h(x)\|^2}, & \text{if } L_g h(x) \neq 0, \\ k_{\rm d}(x), & \text{if } L_g h(x) = 0, \end{cases}$$
$$\eta(x) = -L_f h(x) - L_g h(x) k_{\rm d}(x) - \alpha\big(h(x)\big). \tag{9}$$

A. Motivation: Multiple CBFs

Controller (9) guarantees safety w.r.t. a single safe set $\mathcal{C}$. However, there exist more complex safety specifications in practice that involve compositions of multiple sets. Such general specifications are discussed in the next section. As motivation, we first consider the case of enforcing multiple safety constraints simultaneously, given by the sets:

$$\mathcal{C}_i = \{x \in \mathbb{R}^n : h_i(x) \geq 0\}, \tag{10}$$

and CBF candidates h_i, with $i \in I = \{1, 2, \dots, N\}$. Our goal is to maintain $x(t) \in \mathcal{C}_i\ \forall t \geq 0$ and $\forall i \in I$, that corresponds to rendering the *intersection* of sets $\mathcal{C}_i$ safe.

One may achieve this goal by enforcing multiple constraints on the input simultaneously, for example, by the QP:

$$\begin{aligned} k(x) = \underset{u \in \mathbb{R}^m}{\operatorname{argmin}} \quad & \|u - k_{\rm d}(x)\|^2 \\ \text{s.t.} \quad & \dot{h}_i(x, u) \geq -\alpha_i\big(h_i(x)\big) \quad \forall i \in I. \end{aligned} \tag{11}$$

However, (11) may not be feasible (its solution may not exist) for arbitrary number of constraints. Even if each h_i is CBF and consequently each individual constraint in (11) could be satisfied by a control input, the same input may not satisfy all constraints. For the feasibility of (11) we rather require:

$$\sup_{u \in \mathbb{R}^m} \min_{i \in I} \Big(\dot{h}_i(x, u) + \alpha_i\big(h(x)\big)\Big) \geq 0, \tag{12}$$

cf. (5), that can also be stated in a form like (6) as follows.

Theorem 2. *The QP* (11) *is feasible if and only if:*

$$\sum_{i \in I} \lambda_i L_g h_i(x) = 0 \implies \sum_{i \in I} \lambda_i \Big(L_f h_i(x) + \alpha_i\big(h_i(x)\big)\Big) \geq 0 \tag{13}$$

holds for all $x \in \mathbb{R}^n$ and $\lambda_i \geq 0$.

The proof is given in the Appendix.

This highlights that multiple CBFs are more challenging to use than a single one. With this as motivation, next we propose to encode all safety specifications into a single CBF.

III. COMPLEX SAFETY SPECIFICATIONS

We propose a framework to construct a single CBF candidate that captures complex safety specifications, wherein safety is given by Boolean logical operations between multiple constraints. For example, the motivation above involves logical AND operation: $x(t) \in \mathcal{C}_1$ AND ... AND $x(t) \in \mathcal{C}_N$ must hold. Next, we discuss arbitrary logical compositions (with AND, OR and negation) of safety constraints.

A. Operations Between Sets

Consider multiple safety constraints, each given by a set $\mathcal{C}_i$ in (10). These may be combined via the following Boolean logical operations to capture complex safety specifications.

1) Identity / class-$\mathcal{K}^{\rm e}$ function: The 0-superlevel set $\mathcal{C}_i$ of h_i is the same as that of $\gamma_i \circ h_i$ for any $\gamma_i \in \mathcal{K}^{\rm e}$:

$$\mathcal{C}_i = \{x \in \mathbb{R}^n : \gamma_i\big(h_i(x)\big) \geq 0\}. \tag{14}$$

2) Complement set / negation: The complement[3] $\overline{\mathcal{C}_i}$ of the 0-superlevel set of h_i is the 0-superlevel set of $-h_i$:

$$\overline{\mathcal{C}_i} = \{x \in \mathbb{R}^n : -h_i(x) \geq 0\}. \tag{15}$$

3) Union of sets / maximum / OR operation: The union of multiple 0-superlevel sets:

$$\textstyle\bigcup_{i \in I} \mathcal{C}_i = \{x \in \mathbb{R}^n : \exists i \in I \text{ s.t. } h_i(x) \geq 0\} \tag{16}$$

can be given by a single inequality with the $\max$ function [9]:

$$\textstyle\bigcup_{i \in I} \mathcal{C}_i = \Big\{x \in \mathbb{R}^n : \displaystyle\max_{i \in I} h_i(x) \geq 0\Big\}. \tag{17}$$

The union describes logical OR relation between constraints:

$$x \in \textstyle\bigcup_{i \in I} \mathcal{C}_i \iff x \in \mathcal{C}_1 \text{ OR } x \in \mathcal{C}_2 \ \dots \text{ OR } x \in \mathcal{C}_N. \tag{18}$$

4) Intersection of sets / minimum / AND operation: The intersection of multiple 0-superlevel sets:

$$\textstyle\bigcap_{i \in I} \mathcal{C}_i = \{x \in \mathbb{R}^n : h_i(x) \geq 0 \ \ \forall i \in I\} \tag{19}$$

can be compactly expressed using the $\min$ function [9]:

$$\textstyle\bigcap_{i \in I} \mathcal{C}_i = \Big\{x \in \mathbb{R}^n : \displaystyle\min_{i \in I} h_i(x) \geq 0\Big\}. \tag{20}$$

As in the motivation above, the intersection of sets captures logical AND relation between multiple safety constraints:

$$x \in \textstyle\bigcap_{i \in I} \mathcal{C}_i \iff x \in \mathcal{C}_1 \text{ AND } x \in \mathcal{C}_2 \ \dots \text{ AND } x \in \mathcal{C}_N. \tag{21}$$

[2] In (5)-(6), strict inequality ($>$) can also be required rather than non-strict inequality ($\geq$) to ensure the continuity of the underlying controllers [15].

[3] More precisely, $\overline{\mathcal{C}_i}$ is the closure of the complement of $\mathcal{C}_i$, i.e., it includes the boundary $\partial \mathcal{C}_i$ (where $h_i(x) = 0$).

Further operations between sets can be decomposed into applications of identity, complement, union and intersection, which are represented equivalently by class-$\mathcal{K}^{\rm e}$ functions, negation, $\max$ and $\min$ operations, respectively.

Remark 1. Note that h_i may have various physical meanings and orders of magnitude for different i. Thus, for numerical conditioning (especially when we use exponentials later on), one may scale h_i to $\gamma_i \circ h_i$ with continuously differentiable $\gamma_i \in \mathcal{K}^{\rm e}$. For example, $\gamma_i(r) = \tanh(r)$ scales to the interval $\gamma_i(h_i(x)) \in [-1, 1]$ that may help numerics. Next, we assume that the definitions of h_i already include any necessary scaling and we omit γ_i. Likewise, we do not discuss negation further by assuming that h_i are defined with proper sign.

B. Smooth Approximations to Construct a Single CBF

While the union and intersection of sets are described by a single function in (17) and (20), the resulting expressions, $\max_{i \in I} h_i(x)$ and $\min_{i \in I} h_i(x)$, may not be continuously differentiable in x [9], and they are not CBFs. As main result, we propose a CBF candidate by smooth approximations of $\max$ and $\min$, and describe its properties. This enables us to enforce complex safety specifications as a single constraint.

1) Union of Sets: To capture the union of sets in (17), we propose a CBF candidate via a smooth over-approximation of the $\max$ function using a log-sum-exp expression [13]:

$$h(x) = \frac{1}{\kappa} \ln \Bigg(\sum_{i \in I} {\rm e}^{\kappa h_i(x)} \Bigg) \tag{22}$$

with smoothing parameter $\kappa > 0$. The Lie derivatives are:

$$L_f h(x) {=} \sum_{i \in I} \lambda_i(x) L_f h_i(x), \;\; L_g h(x) {=} \sum_{i \in I} \lambda_i(x) L_g h_i(x), \tag{23}$$

with the coefficients:

$$\lambda_i(x) = {\rm e}^{\kappa (h_i(x) - h(x))}, \tag{24}$$

that satisfy $\sum_{i \in I} \lambda_i(x) = 1$. The proposed CBF candidate in (22) has the properties below; see proof in the Appendix.

Theorem 3. *Consider sets $\mathcal{C}_i$ in* (10) *given by functions h_i, and the union $\bigcup_{i \in I} \mathcal{C}_i$ in* (17)*. Function h in* (22) *over-approximates the* max *expression in* (17) *with bounds:*

$$\max_{i \in I} h_i(x) \leq h(x) \leq \max_{i \in I} h_i(x) + \frac{\ln N}{\kappa} \quad \forall x \in \mathbb{R}^n, \tag{25}$$

such that $\lim_{\kappa \to \infty} h(x) = \max_{i \in I} h_i(x)$. The corresponding set $\mathcal{C}$ in (3) *encapsulates the union, $\mathcal{C} \supseteq \bigcup_{i \in I} \mathcal{C}_i$, such that $\lim_{\kappa \to \infty} \mathcal{C} = \bigcup_{i \in I} \mathcal{C}_i$. Moreover, if* (13) *holds for all $x \in \mathbb{R}^n$ with λ_i in* (24)*, then h is a CBF for* (1) *on $\mathbb{R}^n$ with any $\alpha \in \mathcal{K}^{\rm e}_\infty$ that satisfies $\alpha(r) \geq \alpha_i(r)$ $\forall r \in \mathbb{R}$ and $\forall i \in I$.*

Remark 2. A set $\mathcal{C}$ that *lies inside* the union of the individual sets can also be built by using a buffer b when defining h:

$$h(x) = \frac{1}{\kappa} \ln \Bigg(\sum_{i \in I} {\rm e}^{\kappa h_i(x)} \Bigg) - \frac{b}{\kappa}. \tag{26}$$

For example, based on the upper bound in (25), $b = \ln N$ leads to $h(x) \leq \max_{i \in I} h_i(x)$ and $\mathcal{C} \subseteq \bigcup_{i \in I} \mathcal{C}_i$. Alternatively, buffers from problem-specific bounds that are tighter than (25) can give better inner-approximation $\mathcal{C}$ of $\bigcup_{i \in I} \mathcal{C}_i$.

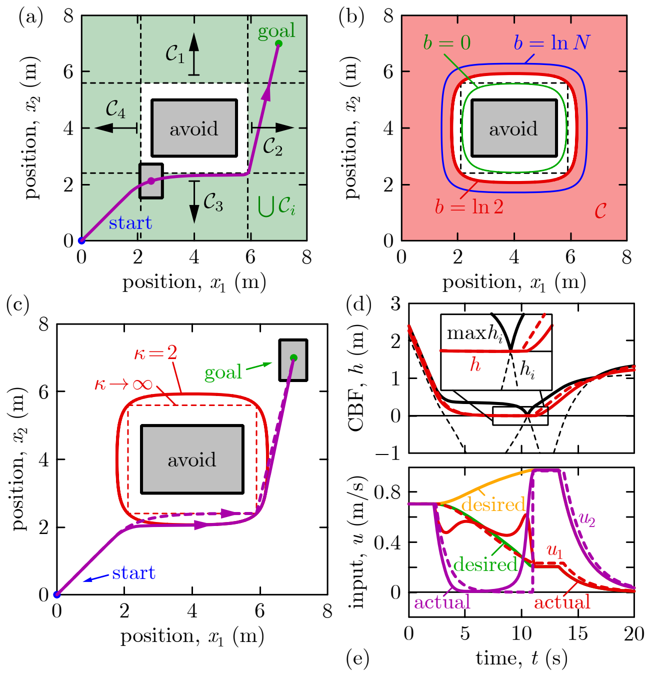

Fig. 1. Numerical results for Example 1, where a reach-avoid task is safely executed. (a) Safe set, (b) 0-superlevel set of the proposed CBF (26), (c)-(e) simulation of safety-critical control by (9).

Example 1. Consider Fig. 1, where a rectangular agent with planar position $x \in \mathbb{R}^2$, velocity $u \in \mathbb{R}^2$, and dynamics:

$$\dot{x} = u \tag{27}$$

is controlled to reach a desired position $x_{\rm d} \in \mathbb{R}^2$ while avoiding a rectangular obstacle[4]. To reach the goal, we use a proportional controller with gain $K_{\rm p} > 0$ and saturation:

$$k_{\rm d}(x) = {\rm sat}\big(K_{\rm p}(x_{\rm d} - x)\big), \tag{28}$$

where ${\rm sat}(u) = \min\{1, u_{\max}/\|u\|_2\} u$ with some $u_{\max} > 0$. We modify this desired controller to a safe controller using the safety filter (9) and the proposed CBF construction.

To avoid the obstacle, the agent's center must be outside a rectangle that has the combined size of the obstacle and the agent; see Fig. 1(a). This means $N = 4$ constraints linked with OR logic: keep the center left to OR above OR right to OR below the rectangle. Accordingly, the safe set is given by the union $\bigcup_{i \in I} \mathcal{C}_i$ of four individual sets $\mathcal{C}_i$ described by four barriers at location $x_i \in \mathbb{R}^2$ with normal vector $n_i \in \mathbb{R}^2$:

$$h_i(x) = n_i^\top (x - x_i), \tag{29}$$

$i \in I = \{1, 2, 3, 4\}$. We combine the four barriers with (26). The resulting safe set $\mathcal{C}$ is plotted in Fig. 1(b) for $\kappa = 2$ and various buffers b. Set $\mathcal{C}$ encapsulates $\bigcup_{i \in I} \mathcal{C}_i$ for $b = 0$, whereas set $\mathcal{C}$ lies inside $\bigcup_{i \in I} \mathcal{C}_i$ for $b = \ln N$; cf. Remark 2. For the problem-specific buffer $b = \ln 2$ (where N is replaced by 2 since two barriers meet at each corner), the approximation $\mathcal{C}$ gets very close to the corners of $\bigcup_{i \in I} \mathcal{C}_i$.

We executed controller (9) with $K_{\rm p} = 0.5$, $u_{\max} = 1$, $\kappa = 2$, $b = \ln 2$ and $\alpha(h) = h$; see solid lines in Fig. 1(c).

[4] Matlab codes for each example are available at: `https://github.com/molnartamasg/CBFs-for-complex-safety-specs`.

The reach-avoid task is successfully accomplished by keeping the agent within set $\mathcal{C}$. Fig. 1(d) highlights that safety is maintained w.r.t. a smooth under-approximation h (red) of the maximum $\max_{i \in I} h_i$ (black) of the individual barriers h_i (dashed). Fig. 1(e) indicates the underlying control input. We also demonstrate by dashed lines in Fig. 1(c)-(e) the case of increasing the smoothing parameter to $\kappa \to \infty$. The sharp corner is recovered and the input becomes discontinuous (u_2 jumps). While discontinuous inputs can be addressed by nontrivial nonsmooth CBF theory [9], they may be difficult to realize accurately by actuators in engineering systems.

2) Intersection of Sets: To capture the intersection of sets in (20), we propose to use a smooth under-approximation of the $\min$ function as CBF candidate [13], analogously to (22):

$$h(x) = -\frac{1}{\kappa} \ln \bigg(\sum_{i \in I} \mathrm{e}^{-\kappa h_i(x)} \bigg). \tag{30}$$

The Lie derivatives of h are expressed by (23) with:

$$\lambda_i(x) = \mathrm{e}^{-\kappa(h_i(x) - h(x))}, \tag{31}$$

that satisfy $\sum_{i \in I} \lambda_i(x) = 1$. The proposed CBF candidate in (30) has the properties below, as proven in the Appendix.

Theorem 4. *Consider sets $\mathcal{C}_i$ in* (10) *given by functions h_i, and the intersection $\bigcap_{i \in I} \mathcal{C}_i$ in* (20). *Function h in* (30) *under-approximates the* $\min$ *expression in* (20) *with bounds:*

$$\min_{i \in I} h_i(x) - \frac{\ln N}{\kappa} \leq h(x) \leq \min_{i \in I} h_i(x) \quad \forall x \in \mathbb{R}^n, \tag{32}$$

such that $\lim_{\kappa \to \infty} h(x) = \min_{i \in I} h_i(x)$. *The corresponding set $\mathcal{C}$ in* (3) *lies inside the intersection, $\mathcal{C} \subseteq \bigcap_{i \in I} \mathcal{C}_i$, such that* $\lim_{\kappa \to \infty} \mathcal{C} = \bigcap_{i \in I} \mathcal{C}_i$.

C. Single CBF for Arbitrary Safe Set Compositions

Having discussed the union and intersection of sets, we extend our framework to arbitrary combinations of unions and intersections. These include e.g. two-level or three-level compositions, like $\bigcup \bigcap_i \mathcal{C}_i$ or $\bigcap \bigcup \bigcap_i \mathcal{C}_i$, etc. We propose an algorithmic way to capture these by a single CBF candidate.

Specifically, consider M levels of safety specifications that establish a single safe set by composing N individual sets. The individual sets are $\mathcal{C}_i$ in (10), $i \in I = \{1, \ldots, N\}$. The specification levels are indexed by $\ell \in L = \{1, \ldots, M\}$. At each level, the union or intersection of sets is taken, resulting in N_ℓ new sets, denoted by $\mathcal{C}_i^\ell$, $i \in I_\ell = \{1, \ldots, N_\ell\}$. This is repeated until a single safe set, called $\mathcal{C}_\mathrm{c}$, is obtained:

$$\begin{aligned}
&\mathcal{C}_i^0 = \mathcal{C}_i, \quad i \in I, \\
&\mathcal{C}_i^\ell = \begin{cases} \bigcup_{j \in J_i^\ell} \mathcal{C}_j^{\ell-1} & \text{if } \ell \in L_\cup, \\ \bigcap_{j \in J_i^\ell} \mathcal{C}_j^{\ell-1} & \text{if } \ell \in L_\cap, \end{cases} \quad i \in I_\ell, \\
&\mathcal{C}_\mathrm{c} = \mathcal{C}_1^M,
\end{aligned} \tag{33}$$

where $J_i^\ell \subseteq I_{\ell-1}$ is the indices of sets that combine into C_i^ℓ, while $L_\cup$ and $L_\cap$ are the indices of levels with union and intersection ($L = L_\cup \cup L_\cap$). Unions and intersections imply the maximum and minimum of the individual barriers h_i, respectively, resulting in the combined CBF candidate h_c [9]:

$$\begin{aligned}
&h_i^0(x) = h_i(x), \quad i \in I, \\
&h_i^\ell(x) = \begin{cases} \max_{j \in J_i^\ell} h_j^{\ell-1}(x) & \text{if } \ell \in L_\cup, \\ \min_{j \in J_i^\ell} h_j^{\ell-1}(x) & \text{if } \ell \in L_\cap, \end{cases} \quad i \in I_\ell, \\
&h_\mathrm{c}(x) = h_1^M(x).
\end{aligned} \tag{34}$$

This describes the safe set (that is assumed to be non-empty):

$$\mathcal{C}_\mathrm{c} = \{x \in \mathbb{R}^n : h_\mathrm{c}(x) \geq 0\}. \tag{35}$$

While the combined function h_c is nonsmooth [9], we propose a continuously differentiable function h, by extending the smooth approximations (22) and (30) of min and max:

$$\begin{aligned}
&H_i^0(x) = \mathrm{e}^{\kappa h_i(x)}, \quad i \in I, \\
&H_i^\ell(x) = \begin{cases} \sum_{j \in J_i^\ell} H_j^{\ell-1}(x) & \text{if } \ell \in L_\cup, \\ \frac{1}{\sum_{j \in J_i^\ell} \frac{1}{H_j^{\ell-1}(x)}} & \text{if } \ell \in L_\cap, \end{cases} \quad i \in I_\ell, \\
&h(x) = \frac{1}{\kappa} \ln H_1^M(x) - \frac{b}{\kappa}.
\end{aligned} \tag{36}$$

Note that we included a buffer b, according to Remark 2, to be able to adjust whether the resulting set $\mathcal{C}$ encapsulates $\mathcal{C}_\mathrm{c}$ or lies inside it. The derivative of the CBF candidate h is:

$$\begin{aligned}
&\dot{H}_i^0(x,u) = \kappa H_i^0(x) \dot{h}_i(x,u), \quad i \in I, \\
&\dot{H}_i^\ell(x,u) = \begin{cases} \sum_{j \in J_i^\ell} \dot{H}_j^{\ell-1}(x,u) & \text{if } \ell \in L_\cup, \\ H_i^\ell(x)^2 \sum_{j \in J_i^\ell} \frac{\dot{H}_j^{\ell-1}(x,u)}{H_j^{\ell-1}(x)^2} & \text{if } \ell \in L_\cap, \end{cases} \quad i \in I_\ell, \\
&\dot{h}(x,u) = \frac{\dot{H}_1^M(x,u)}{\kappa H_1^M(x)}.
\end{aligned} \tag{37}$$

The proposed function h approximates h_c with the following properties that are proven in the Appendix.

Theorem 5. *Consider sets $\mathcal{C}_i$ in* (10) *given by functions h_i, and the composition $\mathcal{C}_\mathrm{c}$ in* (33) *given by h_c in* (34)-(35). *Function h in* (36) *approximates h_c with the error bound:*

$$-\frac{b_\cap + b}{\kappa} \leq h(x) - h_\mathrm{c}(x) \leq \frac{b_\cup - b}{\kappa} \quad \forall x \in \mathbb{R}^n, \tag{38}$$

where $b_\cap = \sum_{\ell \in L_\cap} \ln b_\ell$, $b_\cup = \sum_{\ell \in L_\cup} \ln b_\ell$, $b_\ell = \max_{i \in I_\ell} |J_i^\ell|$, *and $|J_i^\ell|$ is the number of elements in J_i^ℓ. If $b \geq b_\cup$, the corresponding set $\mathcal{C}$ in* (3) *lies inside $\mathcal{C}_\mathrm{c}$, i.e., $\mathcal{C} \subseteq \mathcal{C}_\mathrm{c}$, whereas if $b \leq -b_\cap$, set $\mathcal{C}$ encapsulates $\mathcal{C}_\mathrm{c}$, i.e., $\mathcal{C} \supseteq \mathcal{C}_\mathrm{c}$. Furthermore, we have* $\lim_{\kappa \to \infty} h(x) = h_\mathrm{c}(x)$ *and* $\lim_{\kappa \to \infty} \mathcal{C} = \mathcal{C}_\mathrm{c}$.

The proposed approach in (36) captures complex safety specifications algorithmically by a single CBF candidate h, via the recursive use of (22) and (30) such that exponentials and logarithms are computed only once. Safety is then interpreted w.r.t. set $\mathcal{C}$, which can be tuned to approximate the specified set $\mathcal{C}_\mathrm{c}$ as desired. Based on the error bound (38), increasing κ makes the approximation tighter, while b affects whether $\mathcal{C} \subseteq \mathcal{C}_\mathrm{c}$ or $\mathcal{C} \supseteq \mathcal{C}_\mathrm{c}$. Note that h is a valid CBF only if it satisfies (5). This is not guaranteed by Theorem 5, and it would require additional conditions like (13) in Theorem 3. If h is a CBF, formal safety guarantees can be maintained,

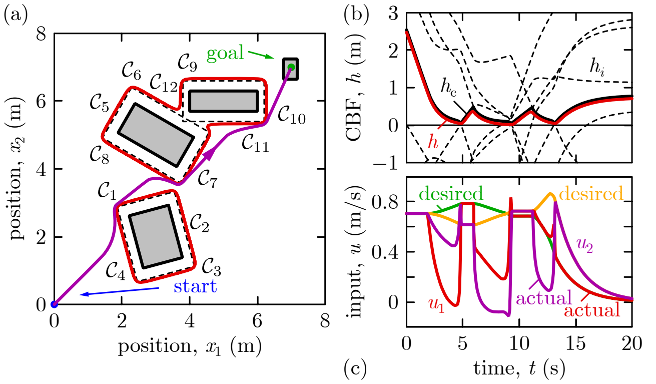

Fig. 2. Numerical results for Example 2, where a reach-avoid task with multiple obstacles is executed by controller (9) with the proposed CBF (36).

for example, by QP (8) that has a single constraint and the explicit solution (9). If the constraint is enforced outside set $\mathcal{C}$, then $\mathcal{C}$ is asymptotically stable; cf. Theorem 1. We remark that, potentially, the log-sum-exp formulas could be replaced by other smooth approximations of max and min. Furthermore, note that computing exponentials may cause numerical issues if κ is too large. These may be alleviated by scaling CBF candidates by class-$\mathcal{K}^{\mathrm{e}}$ functions; see Remark 1.

Example 2. Consider the reach-avoid task of Example 1, with dynamics (27), desired controller (28), safety filter (9), and multiple obstacles shown in Fig. 2. Like in Example 1, each of the three obstacles yields four safety constraints, leading to $N = 12$ sets $\mathcal{C}_i$ and functions h_i, given by (29). The four constraints of each obstacle are linked with OR logic, like in Example 1, while the constraints of different obstacles are linked with AND: safety is maintained w.r.t. obstacle 1 AND obstacle 2 AND obstacle 3. Thus, the safe set:

$$\mathcal{C}_{\mathrm{c}} = (\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4) \cap (\mathcal{C}_5 \cup \mathcal{C}_6 \cup \mathcal{C}_7 \cup \mathcal{C}_8) \cap (\mathcal{C}_9 \cup \mathcal{C}_{10} \cup \mathcal{C}_{11} \cup \mathcal{C}_{12}) \tag{39}$$

is given by a $M = 2$ level specification, combining $N = 12$ sets to $N_1 = 3$ sets ($\mathcal{C}_1^1$ from sets given by $J_1^1 = \{1, 2, 3, 4\}$, $\mathcal{C}_2^1$ from $J_2^1 = \{5, 6, 7, 8\}$ and $\mathcal{C}_3^1$ from $J_3^1 = \{9, 10, 11, 12\}$), and then to a single set $\mathcal{C}_{\mathrm{c}}$ (via sets given by $J_1^2 = \{1, 2, 3\}$).

The behavior of controller (9) with the proposed CBF candidate (36) is shown in Fig. 2 for $K_{\mathrm{p}} = 0.5$, $u_{\max} = 1$, $\kappa = 10$, $b = \ln 2$ and $\alpha(h) = h$. The reach-avoid task is successfully accomplished with formal guarantees of safety. Remarkably, the controller is continuous and explicit, since the control law (9) and CBF formulas (36)-(37) are in closed form. Such explicit controllers are easy to implement and fast to execute. Note that controller (11) could also handle multiple obstacles if each obstacle was given by a single CBF candidate. Yet, (11) cannot address multi-level safety specifications like (39), while the proposed method can.

Example 3. Consider the setup of Fig. 3 where a point agent is driven to a desired location while staying on a road network, with dynamics (27), desired controller (28) and safety-critical controller (9). Safety is determined by the road geometry. Each road boundary is related to a set, which is given for straight roads by (29) and for ring roads by:

$$h_i(x) = \pm\big(\|x - x_i\| - R_i\big). \tag{40}$$

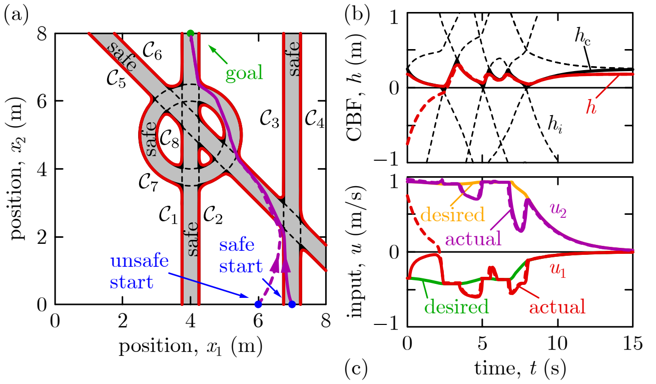

Fig. 3. Numerical results for Example 3, where an agent is driven safely along a road network via controller (9) with the proposed CBF (36).

Here plus and minus signs stand for the inner and outer circles, respectively, R_i is their radius, and x_i is their center. Safety must be ensured w.r.t. boundary 1 AND boundary 2 of each road, while the agent must stay on road 1 OR road 2 OR road 3 OR road 4. Thus, the combined safe set becomes:

$$\mathcal{C}_{\mathrm{c}} = (\mathcal{C}_1 \cap \mathcal{C}_2) \cup (\mathcal{C}_3 \cap \mathcal{C}_4) \cup (\mathcal{C}_6 \cap \mathcal{C}_5) \cup (\mathcal{C}_7 \cap \mathcal{C}_8). \tag{41}$$

That is, we have a $M = 2$ level specification with $N = 8$ sets combined first to $N_1 = 4$ sets (as intersections of sets given by $J_1^1 = \{1, 2\}$, $J_2^1 = \{3, 4\}$, $J_3^1 = \{5, 6\}$, $J_4^1 = \{7, 8\}$), and then to a single set (as union via $J_1^2 = \{1, 2, 3, 4\}$).

The execution of the reach-avoid task with the proposed CBF candidate (36) and controller (9) is shown in Fig. 3 for $K_{\mathrm{p}} = 0.5$, $u_{\max} = 1$, $\kappa = 10$, $b = 0$ and $\alpha(h) = h$. The end result is guaranteed safety (see solid lines). Moreover, the safe set is attractive: in case of an unsafe, off-road initial condition the agent returns to to the safe set on the road and continues to be safe (see thick dashed lines). Remarkably, this property was not provided by earlier works like [11].

IV. CONCLUSION

We established a framework to capture complex safety specifications by control barrier functions (CBFs). The specifications are combinations of state constraints by Boolean logic. We proposed an algorithmic way to create a single CBF candidate that encodes these constraints and enables efficient safety-critical controllers. We described the properties of this CBF candidate, and we used simulations to show its ability to tackle nontrivial safety-critical control problems.

APPENDIX

Proof of Theorem 2. Consider the Lagrangian of the feasibility problem [18] corresponding to the QP (11):

$$L(x, u, \lambda) = -\sum_{i \in I} \lambda_i \Big(\dot{h}_i(x, u) + \alpha_i\big(h(x)\big)\Big), \tag{42}$$

with the Lagrange multipliers $\lambda = \begin{bmatrix}\lambda_1 & \lambda_2 & \dots & \lambda_N\end{bmatrix}^\top$, $\lambda_i \geq 0$ $\forall i \in I$. The QP (11) is feasible if and only if $\exists u \in \mathbb{R}^m$ such that $L(x, u, \lambda) \leq 0$ $\forall \lambda_i \geq 0$. With the Lagrange dual function, $g_L(x, \lambda) = \inf_{u \in \mathbb{R}^m} L(x, u, \lambda)$, this means $g_L(x, \lambda) \leq 0$ $\forall \lambda_i \geq 0$. Since $g_L(x, \lambda) = -\sum_{i \in I} \lambda_i \Big(L_f h_i(x) + \alpha_i\big(h_i(x)\big)\Big)$ if $\sum_{i \in I} \lambda_i L_g h_i(x) = 0$ and $g_L(x, \lambda) = -\infty$ otherwise, (13) is equivalent to $g_L(x, \lambda) \leq 0$ and provides feasibility. □

Proof of Theorem 3. Since the exponential function is monotonous and gives positive value, we have:

$$\mathrm{e}^{\kappa \max_{i\in I} h_i(x)} \leq \sum_{i\in I} \mathrm{e}^{\kappa h_i(x)} \leq N\mathrm{e}^{\kappa \max_{i\in I} h_i(x)}, \tag{43}$$

that yields (25) via (22) and the monotonicity of $\ln$. The limit on both sides of (25) yields $\lim_{\kappa\to\infty} h(x) = \max_{i\in I} h_i(x)$, and consequently $\lim_{\kappa\to\infty} \mathcal{C} = \bigcup_{i\in I} \mathcal{C}_i$ holds. Due to (25), $\max_{i\in I} h_i(x) \geq 0 \implies h(x) \geq 0$, therefore $x \in \bigcup_{i\in I} \mathcal{C}_i \implies x \in \mathcal{C}$, and $\mathcal{C} \supseteq \bigcup_{i\in I} \mathcal{C}_i$ follows.

We prove that h is a CBF by showing that (6) holds. We achieve this by relating $L_g h(x)$ and $L_f h(x) + \alpha\big(h(x)\big)$ to $L_g h_i(x)$ and $L_f h_i(x) + \alpha_i\big(h_i(x)\big)$. The Lie derivatives are related by (23), while the following bound holds for all $i \in I$:

$$\alpha\big(h(x)\big) \geq \alpha\big(h_i(x)\big) \geq \alpha_i\big(h_i(x)\big), \tag{44}$$

where we used (25) and $\alpha(r) \geq \alpha_i(r)$. Consequently, since $\sum_{i\in I} \lambda_i(x) = 1$ and $\lambda_i(x) > 0$ hold via (24), we have:

$$L_f h(x) + \alpha\big(h(x)\big) \geq \sum_{i\in I} \lambda_i(x) \Big(L_f h_i(x) + \alpha_i\big(h_i(x)\big)\Big). \tag{45}$$

If $L_g h(x) = 0$, we get $\sum_{i\in I} \lambda_i(x) L_g h_i(x) = 0$ based on (23), and since (13) is assumed to hold, (45) finally yields $L_f h(x) + \alpha\big(h(x)\big) \geq 0$. Thus, (6) holds and h is a CBF. □

Proof of Theorem 4. The proof follows that of Theorem 3, with the following modifications. We replace (43) by:

$$\mathrm{e}^{-\kappa \min_{i\in I} h_i(x)} \leq \sum_{i\in I} \mathrm{e}^{-\kappa h_i(x)} \leq N\mathrm{e}^{-\kappa \min_{i\in I} h_i(x)}, \tag{46}$$

that gives the bound (32) via (30). The remaining properties follow from the limit on both sides of (32) and from $h(x) \geq 0 \implies \min_{i\in I} h_i(x) \geq 0$ according to (32). □

Proof of Theorem 5. By leveraging that the exponential function is monotonous, we write (34) equivalently as:

$$\begin{aligned}
H^0_{\mathrm{c},i}(x) &= \mathrm{e}^{\kappa h_i(x)}, \quad i \in I, \\
H^\ell_{\mathrm{c},i}(x) &= \begin{cases} \max_{j\in J_i^\ell} H^{\ell-1}_{\mathrm{c},j}(x) & \text{if } \ell \in L_\cup, \\ \min_{j\in J_i^\ell} H^{\ell-1}_{\mathrm{c},j}(x) & \text{if } \ell \in L_\cap, \end{cases} \quad i \in I_\ell, \\
h_\mathrm{c}(x) &= \frac{1}{\kappa} \ln H^M_{\mathrm{c},1}(x).
\end{aligned} \tag{47}$$

We compare this with the definition (36) of h. First, by using the middle row of (36), we establish that for all $x \in \mathbb{R}^n$:

$$\begin{aligned}
&H^{\ell-1}_j(x) \leq H^\ell_i(x) \leq |J_i^\ell| \max_{j\in J_i^\ell} H^{\ell-1}_j(x) \quad \text{if } \ell \in L_\cup, \\
&\frac{1}{|J_i^\ell|} \min_{j\in J_i^\ell} H^{\ell-1}_j(x) \leq H^\ell_i(x) \leq H^{\ell-1}_j(x) \quad \text{if } \ell \in L_\cap
\end{aligned} \tag{48}$$

$\forall j \in J_i^\ell$ and $\forall i \in I_\ell$. Then, we relate $H^\ell_{\mathrm{c},i}$ to H^ℓ_i by induction. For $\ell \geq 1$ we assume that there exist $\underline{c}_{\ell-1}, \overline{c}_{\ell-1} > 0$ such that:

$$\underline{c}_{\ell-1} H^{\ell-1}_{\mathrm{c},i}(x) \leq H^{\ell-1}_i(x) \leq \overline{c}_{\ell-1} H^{\ell-1}_{\mathrm{c},i}(x) \tag{49}$$

$\forall x \in \mathbb{R}^n$ and $\forall i \in I_{\ell-1}$. This is true for $\ell = 1$ with $\underline{c}_0, \overline{c}_0 = 1$ since $H^0_i(x) = H^0_{\mathrm{c},i}(x)$. By substituting (49) into (48), using the middle row of (47) and $|J_i^\ell| \leq \max_{i\in I_\ell} |J_i^\ell|$, we get:

$$\underline{c}_\ell H^\ell_{\mathrm{c},i}(x) \leq H^\ell_i(x) \leq \overline{c}_\ell H^\ell_{\mathrm{c},i}(x) \tag{50}$$

with $b_\ell = \max_{i\in I_\ell} |J_i^\ell|$ and:

$$\underline{c}_\ell = \begin{cases} \underline{c}_{\ell-1} & \text{if } \ell \in L_\cup, \\ \frac{\underline{c}_{\ell-1}}{b_\ell} & \text{if } \ell \in L_\cap, \end{cases} \qquad \overline{c}_\ell = \begin{cases} b_\ell \overline{c}_{\ell-1} & \text{if } \ell \in L_\cup, \\ \overline{c}_{\ell-1} & \text{if } \ell \in L_\cap. \end{cases} \tag{51}$$

By induction, (50) holds for $\ell = M$ with $\underline{c}_M = \prod_{\ell\in L_\cap} \frac{1}{b_\ell}$ and $\overline{c}_M = \prod_{\ell\in L_\cup} b_\ell$. Taking the logarithm of (50) with $\ell = M$ and using the last rows of (36) and (47) result in (38). □

References

[1] 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.

[2] M. Rauscher, M. Kimmel, and S. Hirche, "Constrained robot control using control barrier functions," in *IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2016, pp. 279–285.

[3] X. Xu, "Constrained control of input–output linearizable systems using control sharing barrier functions," *Automatica*, vol. 87, pp. 195–201, 2018.

[4] W. Shaw Cortez, X. Tan, and D. V. Dimarogonas, "A robust, multiple control barrier function framework for input constrained systems," *IEEE Control Systems Letters*, vol. 6, pp. 1742–1747, 2022.

[5] X. Tan and D. V. Dimarogonas, "Compatibility checking of multiple control barrier functions for input constrained systems," in *61st IEEE Conference on Decision and Control*, 2022, pp. 939–944.

[6] J. Breeden and D. Panagou, "Compositions of multiple control barrier functions under input constraints," in *American Control Conference*, 2023, pp. 3688–3695.

[7] L. Liu, Y.-J. Liu, D. Li, S. Tong, and Z. Wang, "Barrier Lyapunov function-based adaptive fuzzy FTC for switched systems and its applications to resistance–inductance–capacitance circuit system," *IEEE Transactions on Cybernetics*, vol. 50, no. 8, pp. 3491–3502, 2020.

[8] L. Liu, W. Zhao, Y.-J. Liu, S. Tong, and Y.-Y. Wang, "Adaptive finite-time neural network control of nonlinear systems with multiple objective constraints and application to electromechanical system," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 12, pp. 5416–5426, 2021.

[9] P. Glotfelter, J. Cortés, and M. Egerstedt, "Nonsmooth barrier functions with applications to multi-robot systems," *IEEE Control Systems Letters*, vol. 1, no. 2, pp. 310–315, 2017.

[10] ——, "A nonsmooth approach to controller synthesis for Boolean specifications," *IEEE Transactions on Automatic Control*, vol. 66, no. 11, pp. 5160–5174, 2021.

[11] L. Wang, A. D. Ames, and M. Egerstedt, "Multi-objective compositions for collision-free connectivity maintenance in teams of mobile robots," in *55th IEEE Conference on Decision and Control*, 2016, pp. 2659–2664.

[12] M. Black and D. Panagou, "Adaptation for validation of a consolidated control barrier function based control synthesis," *arXiv preprint*, no. arXiv:2209.08170, 2022.

[13] L. Lindemann and D. V. Dimarogonas, "Control barrier functions for signal temporal logic tasks," *IEEE Control Systems Letters*, vol. 3, no. 1, pp. 96–101, 2019.

[14] ——, "Control barrier functions for multi-agent systems under conflicting local signal temporal logic tasks," *IEEE Control Systems Letters*, vol. 3, no. 3, pp. 757–762, 2019.

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

[16] X. Xu, P. Tabuada, J. W. Grizzle, and A. D. Ames, "Robustness of control barrier functions for safety critical control," in *IFAC Conference on Analysis and Design of Hybrid Systems*, vol. 48, no. 27, 2015, pp. 54–61.

[17] A. Alan, A. J. Taylor, C. R. He, A. D. Ames, and G. Orosz, "Control barrier functions and input-to-state safety with application to automated vehicles," *IEEE Transactions on Control Systems Technology*, vol. 31, no. 6, pp. 2744–2759, 2023.

[18] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge University Press, 2004.