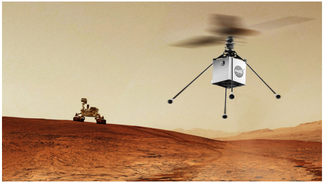
Barrier Functions: Bridging the Gap between Planning from Specifications and Safety-Critical Control

Petter Nilsson and Aaron D. Ames

Department of Mechanical and Civil Engineering
California Institute of Technology

December 17, 2018

Specifications in Control

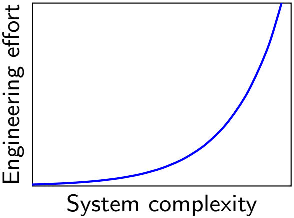


How do we make systems **safe and reliable** as system **complexity and interconnectivity grows**?

Specifications:

- Succinct and precise way to define system behavior
- Facilitate system modularity and interconnections
- **Synthesis algorithms** convert specifications into controllers

Specifications in Control

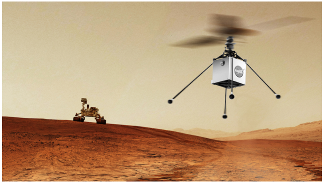


How do we make systems **safe and reliable** as system **complexity and interconnectivity grows**?

Specifications:

- Succinct and precise way to define system behavior
- Facilitate system modularity and interconnections
- **Synthesis algorithms** convert specifications into controllers

Specifications in Control



How do we make systems **safe and reliable** as system **complexity and interconnectivity grows**?

Specifications:

- Succinct and precise way to define system behavior
- Facilitate system modularity and interconnections
- **Synthesis algorithms** convert specifications into controllers

Specifications: Low-level vs High-level

	Low-level	High-level
Time scale	Short	Long
Specification	Invariance-driven	Assume/guarantee-driven
Model	Nonlinear ODE	Abstract model
Methods	HJB[1], SoS[2], CBF[3]	LTL synth[4], MDPs[5]
Decisions	Smooth	Discrete
Dimensionality	High	Low
Uncertainty	Model, perception	Environment
Human analogy	Spinal cord	Brain

Full space gridding intractable for many high-dimensional systems

Need sparse high-level abstractions

[**Among others**: [1]Tomlin, [2]Korda&Henrion, [3]Ames et al, [4]Kress-Gazit, Tabuada, [5]Bertsekas]

Specifications: Low-level vs High-level

	Low-level	High-level
Time scale	Short	Long
Specification	Invariance-driven	Assume/guarantee-driven
Model	Nonlinear ODE	Abstract model
Methods	HJB[1], SoS[2], CBF[3]	LTL synth[4], MDPs[5]
Decisions	Smooth	Discrete
Dimensionality	High	Low
Uncertainty	Model, perception	Environment
Human analogy	Spinal cord	Brain

Full space gridding intractable for many high-dimensional systems

Need sparse high-level abstractions

[**Among others**: [1]Tomlin, [2]Korda&Henrion, [3]Ames et al, [4]Kress-Gazit, Tabuada, [5]Bertsekas]

Specifications: Low-level vs High-level

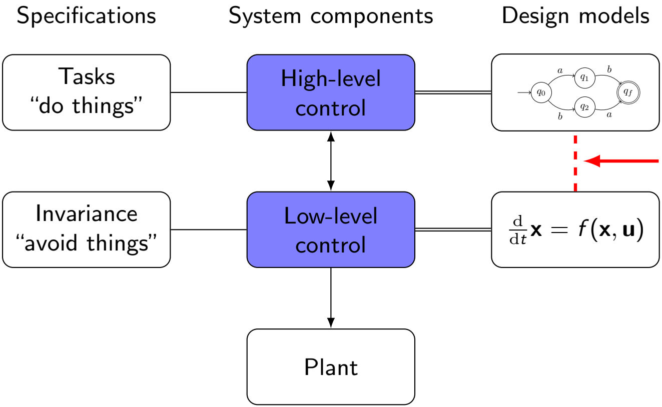
	Low-level	High-level
Time scale	Short	Long
Specification	Invariance-driven	Assume/guarantee-driven
Model	Nonlinear ODE	Abstract model
Methods	HJB[1], SoS[2], CBF[3]	LTL synth[4], MDPs[5]
Decisions	Smooth	Discrete
Dimensionality	High	Low
Uncertainty	Model, perception	Environment
Human analogy	Spinal cord	Brain

Full space gridding intractable for many high-dimensional systems

Need sparse high-level abstractions

[**Among others**: [1]Tomlin, [2]Korda&Henrion, [3]Ames et al, [4]Kress-Gazit, Tabuada, [5]Bertsekas]

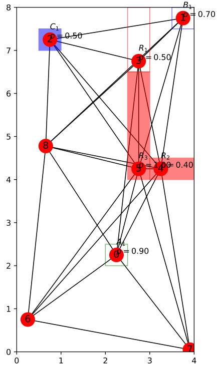
Bridging the Gap



Guarantees when planning on an Abstract Roadmap?

How to relate a low-dimensional roadmap to a high-fidelity model?

- Road map consists of nodes and edges
- Approach: equip graph edges with **certificates for invariance and reachability**
    - Invariance for low-level safety
    - Reachability for high-level/low-level connection



Control Systems and Transition Systems

- $\Sigma = (\mathcal{X}, \mathcal{X}_0, \mathcal{U}, \mathcal{D}, f, h_\mathcal{X})$ is a **control system** over a continuous space $\mathcal{X}$

$$\dot{x} = f(x, u, d), \quad x \in \mathcal{X},\ u \in \mathcal{U},\ d \in \mathcal{D},\ h_\mathcal{X} \text{ output map.}$$

- $\mathcal{T} = (\mathbb{X}, \mathbb{X}_0, \mathbb{U}, \longrightarrow, h_\mathbb{X})$ is a **transition system** over discrete space $\mathbb{X}$

$$\xi \xrightarrow{\mu} \xi', \quad \xi \in \mathbb{X},\ \mu \in \mathbb{U},\ h_\mathbb{X} \text{ output map.}$$

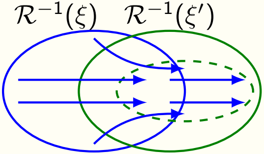
Objective

Construct **abstraction** $\mathcal{T}$ embedded in a **lower dimension** so that a policy for $\mathcal{T}$ can be implemented on Σ.

Alternating Simulation Relation for Planning

Definition

$\mathcal{R} \subset \mathcal{X} \times \mathbb{X}$ is an **alternating planning relation** from Σ to $\mathcal{T}$ if:



1. For all $x_0 \in \mathcal{X}_0$ there exists $\xi_0 \in \mathbb{X}_0$ such that $x_0 \mathcal{R} \xi_0$,
2. For $x \mathcal{R} \xi$, $h_{\mathcal{X}}(x) \in h_{\mathbb{X}}(\xi)$,
3. For $\xi \in \mathbb{X}$ and $\mu \in \mathbb{U}$ there **exists a feedback controller** $u(t, x)$ such that the resulting u-controlled trajectory $\mathbf{x}(t)$ for some T satisfies

$$\mathbf{x}(T) \in \bigcup_{\xi' : \xi \xrightarrow{\mu} \xi'} \mathcal{R}^{-1}(\xi'), \qquad \mathbf{x}([0, T)) \subset \mathcal{R}^{-1}(\xi) \cup \bigcup_{\xi' : \xi \xrightarrow{\mu} \xi'} \mathcal{R}^{-1}(\xi').$$

We say that $\mathcal{T}$ **simulates** Σ and write $\Sigma \preceq_{\text{plan}} \mathcal{T}$.

Relation Preserves LTL Satisfiability

LTL notation:

- Specification: φ
- Transition system $\mathcal{T}$ controlled by policy $\pi_{\mathcal{T}}$ satisfies specification: $(\mathcal{T}, \pi_{\mathcal{T}}) \models \varphi$
- Closed-loop control system satisfies specification: $(\Sigma, \pi_{\Sigma}) \models \varphi$

Theorem

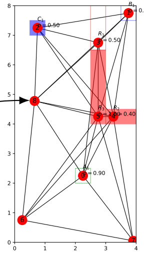
If $\Sigma \preceq_{\text{plan}} \mathcal{T}$ and $\pi_{\mathcal{T}}$ is a policy such that $(\mathcal{T}, \pi_{\mathcal{T}}) \models \varphi$, then there exists a controller π_{Σ} for Σ such that $(\Sigma, \pi_{\Sigma}) \models \varphi$.

Proof: Construct **hybrid event-driven** controller...

Embedding Abstraction in Lower Dimension

Planning space $\mathbf{x} \in \mathcal{X}$ and **higher-order space $\mathbf{v} \in \mathcal{V}$**:

$$\Sigma : \left\{ \frac{\mathrm{d}}{\mathrm{d}t} \begin{bmatrix} \mathbf{x} \\ \mathbf{v} \end{bmatrix} = f(\mathbf{x}, \mathbf{v}) + g_u(\mathbf{x}, \mathbf{v})\mathbf{u} + g_d(\mathbf{x}, \mathbf{v})\mathbf{d} \right.$$



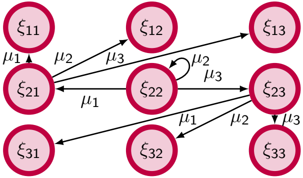
Road map from subsets $\{X_i\} \subset \mathcal{X}$:

- Nodes correspond to sets $\{X_i\}$
- Edges correspond to pairs of sets (X_i, X_j)

Abstract states $\xi_{ij} \in \mathbb{X}$ correspond to edges

ξ_{ij} : transitioning from X_i to X_j

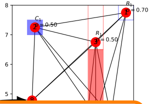
ξ_{ii} : X_i being kept invariant



Embedding Abstraction in Lower Dimension

Planning space $\mathbf{x} \in \mathcal{X}$ and **higher-order space $\mathbf{v} \in \mathcal{V}$**:

$$\Sigma : \left\{ \frac{\mathrm{d}}{\mathrm{d}t} \begin{bmatrix} \mathbf{x} \\ \mathbf{v} \end{bmatrix} = f(\mathbf{x}, \mathbf{v}) + g_u(\mathbf{x}, \mathbf{v})\mathbf{u} + g_d(\mathbf{x}, \mathbf{v})\mathbf{d} \right.$$

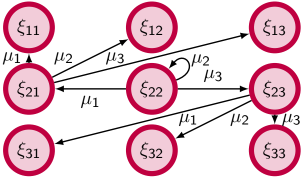


How to ensure **reachability and invariance** in planning space?

Abstract states $\xi_{ij} \in \mathbb{X}$ correspond to edges

ξ_{ij} : transitioning from X_i to X_j

ξ_{ii} : X_i being kept invariant



Control Barrier Function Certificates

X_i can be kept **invariant** if $\exists h_i^{\mathrm{inv}}(x, v), \kappa_i^{\mathrm{inv}} \in \mathcal{K}_\infty$ such that $\forall x, v$

$$h_i^{\mathrm{inv}}(x, v) \geq 0 \implies x \in X_i,$$
$$\kappa_i^{\mathrm{inv}}(h_i^{\mathrm{inv}}(x, v)) + \max_{u \in \mathcal{U}} \min_{d \in \mathcal{D}} \mathcal{L} h_i^{\mathrm{inv}}(x, v, u, d) \geq 0.$$

X_j can be **reached** from X_i if $\exists h_{ij}^{\mathrm{rch}}, \kappa_{ij}^{\mathrm{rch}}, T_{ij}$ such that $\forall x, v$

$$h_i^{\mathrm{inv}}(x, v) \geq 0 \implies h_{ij}^{\mathrm{rch}}(0, x, v) \geq 0,$$
$$h_{ij}^{\mathrm{rch}}(T_{ij}, x, v) \geq 0 \implies h_j^{\mathrm{inv}}(x, v) \geq 0,$$
$$\kappa_{i,j}^{\mathrm{rch}}(h_{ij}^{\mathrm{rch}}(t, x, v)) + \max_{u \in \mathcal{U}} \min_{d \in \mathcal{D}} \mathcal{L} h_{ij}^{\mathrm{rch}}(t, x, v, u, d) \geq 0.$$

Ames et al. TAC'17

Control Barrier Function Certificates

X_i can be kept **invariant** if $\exists h_i^{\mathrm{inv}}(x, v), \kappa_i^{\mathrm{inv}} \in \mathcal{K}_\infty$ such that $\forall x, v$

$$h_i^{\mathrm{inv}}(x, v) \geq 0 \implies x \in X_i,$$

$$\boxed{\kappa_i^{\mathrm{inv}}(h_i^{\mathrm{inv}}(x, v)) + \max_{u \in \mathcal{U}} \min_{d \in \mathcal{D}} \mathcal{L} h_i^{\mathrm{inv}}(x, v, u, d) \geq 0.}$$

X_j can be **reache**

$h_i^{\mathrm{inv}}(x, v) \geq$

$h_{ij}^{\mathrm{rch}}(T_{ij}, x,$

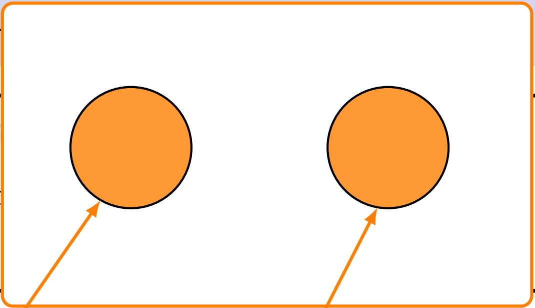
$$\kappa_{i,j}^{\mathrm{rch}}(h_{ij}^{\mathrm{rch}}(t, x, v)) + \max_{u \in \mathcal{U}} \min_{d \in \mathcal{D}} \mathcal{L} h_{ij}^{\mathrm{rch}}(t, x, v, u, d) \geq 0.$$

Exists u such that for all d,

$$\frac{\mathrm{d} h_i^{\mathrm{inv}}(x, v)}{\mathrm{d} t} \geq -\kappa_i^{\mathrm{inv}}(h_i^{\mathrm{inv}}(x, v))$$

Ames et al. TAC'17

Control Barrier Func



X_i can be kept **invar**

$$h_i^{\mathrm{inv}}(x, v) \geq$$
$$\kappa_i^{\mathrm{inv}}(h_i^{\mathrm{inv}}(x,$$

X_j can be **reached** from X_i if $\exists h_{ij}^{\mathrm{rch}}, \kappa_{ij}^{\mathrm{rch}}, T_{ij}$ such that $\forall x, v$

$$\boxed{h_i^{\mathrm{inv}}(x, v) \geq 0} \implies h_{ij}^{\mathrm{rch}}(0, x, v) \geq 0,$$
$$h_{ij}^{\mathrm{rch}}(T_{ij}, x, v) \geq 0 \implies \boxed{h_j^{\mathrm{inv}}(x, v) \geq 0,}$$
$$\kappa_{i,j}^{\mathrm{rch}}(h_{ij}^{\mathrm{rch}}(t, x, v)) + \max_{u \in \mathcal{U}} \min_{d \in \mathcal{D}} \mathcal{L} h_{ij}^{\mathrm{rch}}(t, x, v, u, d) \geq 0.$$

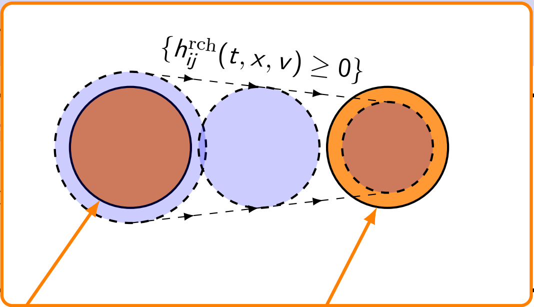
Ames et al. TAC'17

Control Barrier Func

X_i can be kept **invar**

$h_i^{\mathrm{inv}}(x, v) \geq$

$\kappa_i^{\mathrm{inv}}(h_i^{\mathrm{inv}}(x,$



X_j can be **reached** from X_i if $\exists h_{ij}^{\mathrm{rch}}, \kappa_{ij}^{\mathrm{rch}}, T_{ij}$ such that $\forall x, v$

$$\boxed{h_i^{\mathrm{inv}}(x, v) \geq 0} \implies h_{ij}^{\mathrm{rch}}(0, x, v) \geq 0,$$
$$h_{ij}^{\mathrm{rch}}(T_{ij}, x, v) \geq 0 \implies \boxed{h_j^{\mathrm{inv}}(x, v) \geq 0},$$
$$\kappa_{i,j}^{\mathrm{rch}}(h_{ij}^{\mathrm{rch}}(t, x, v)) + \max_{u \in \mathcal{U}} \min_{d \in \mathcal{D}} \mathcal{L} h_{ij}^{\mathrm{rch}}(t, x, v, u, d) \geq 0.$$

Ames et al. TAC'17

Abstraction Satisfies Simulation Relation

For a road map $\mathcal{T}$ where **each edge and node has a certificate**, consider relation $\mathcal{R}$

$$
\begin{aligned}
(x, v)\mathcal{R}\xi_{ii} &\iff h_i^{\mathrm{inv}}(x, v) \geq 0, \\
(x, v)\mathcal{R}\xi_{ij} &\iff \exists t \in [0, T_{ij}] \text{ s.t. } h_{ij}^{\mathrm{rch}}(t, x, v) \geq 0.
\end{aligned}
$$

Theorem

Assume that $\mathcal{X}_0 \subset \bigcup_{\xi \in \mathbb{X}_0} \mathcal{R}^{-1}(\xi)$. Then $\mathcal{R}$ is an alternating planning relation from Σ to $\mathcal{T}$ and thus $\Sigma \preceq_{\mathrm{plan}} \mathcal{T}$.

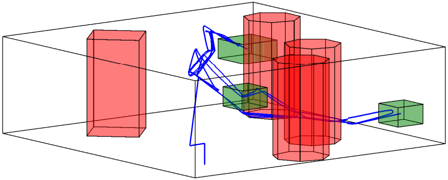
Example: Quadrotor Planning

12D Quadrotor dynamics:

$$\Sigma: \begin{cases} m\ddot{\mathbf{r}} = -mge_z + \mathbf{F}_w R(\xi) e_z \\ \dot{\xi} = T(\xi)\Omega \\ J\dot{\Omega} = \tau - \Omega \times J\Omega \end{cases}$$

3D-embedded road map $\mathcal{T}$

Environment:



Surveillance specification

$$\varphi = \Box \neg D \bigwedge_{i=1}^{3} \Box \Diamond C_i$$

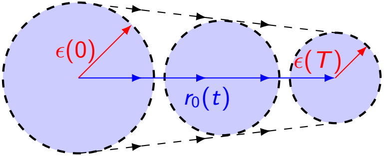
"Avoid danger and always eventually visit target regions"

Trajectory-Centric Certificates for Quadrotor

- Invariance CBF for $\{\|r - r_0(t)\| \leq \epsilon(t)\}$ (if control unbounded):

$$h_0(t, r, \xi) = \epsilon(t)^2(1-\beta) - \|r - r_0(t)\|^2 - \frac{\epsilon^2\beta}{\pi/2} a_1 \arctan\left(a_2(r - r_0(t))^T R(\xi) e_3 + a_3\right).$$

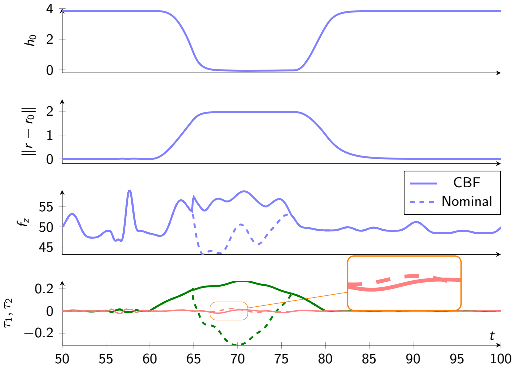
- Reachability CBFs by interpolating $r_0(t)$ and $\epsilon(t)$:



[Wu & Sreenath, Safety-Critical Control of a 3D Quadrotor With Range-Limited Sensing, DSCC'16]

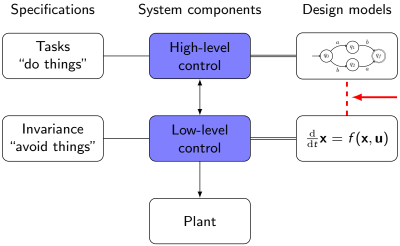
Example: Results

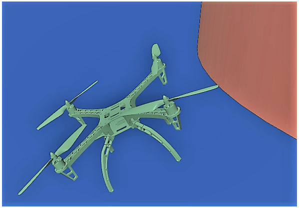
CBFs designed to stay within 2m of nominal path.



CBF conditions **activated in wind disturbance**

Summary





- **Planning** and LTL synthesis in low dimension, **safety** w.r.t. high-fidelity model
    - Quadrotor example: **12D model, 3D planning**
- **Planning relation** as **contract** to relate control system to roadmap
    - Enforce **task specifications on full model**
- **Control barrier functions** as edge certificates
    - CBFs also enforce **safety specifications on full model**

Thank you