MITSUBISHI ELECTRIC RESEARCH LABORATORIES
https://www.merl.com

Projection-free computation of robust controllable sets with constrained zonotopes

Vinod, Abraham P.; Weiss, Avishai; Di Cairano, Stefano

TR2025-023 March 05, 2025

Abstract

We study the problem of computing robust controllable sets for discrete-time linear systems with additive uncertainty. We propose a tractable and scalable approach to inner- and outer-approximate robust controllable sets using constrained zonotopes, when the additive uncertainty set is a symmetric, convex, and compact set. Our least-squares-based approach uses novel closed- form approximations of the Pontryagin difference between a constrained zonotopic minuend and a symmetric, convex, and compact subtrahend. We obtain these approximations using two novel canonical representations for full-dimensional constrained zonotopes. Unlike existing approaches, our approach does not rely on convex optimization solvers, and is projection-free for ellipsoidal and zonotopic uncertainty sets. We also propose a least-squares-based approach to compute a convex, polyhedral outer-approximation to constrained zonotopes, and characterize sufficient conditions under which all these approximations are exact. We demonstrate the computational efficiency and scalability of our approach in several case studies, including the design of abort-safe rendezvous trajectories for a spacecraft in near-rectilinear halo orbit under uncertainty. Our approach can inner-approximate a 20-step robust controllable set for a 100-dimensional linear system in under 15 seconds on a standard computer.

Automatica 2025

© 2025 Licensed under the Creative Commons BY-NC-ND 4.0 license http://creativecommons.org/licenses/by-nc-nd/4.0/.

Mitsubishi Electric Research Laboratories, Inc.
201 Broadway, Cambridge, Massachusetts 02139

Projection-free computation of robust controllable sets with constrained zonotopes ⋆

Abraham P. Vinod [a], Avishai Weiss [a], Stefano Di Cairano [a]

[a] *Mitsubishi Electric Research Laboratories, Cambridge, MA*

Abstract

We study the problem of computing robust controllable sets for discrete-time linear systems with additive uncertainty. We propose a tractable and scalable approach to inner- and outer-approximate robust controllable sets using constrained zonotopes, when the additive uncertainty set is a symmetric, convex, and compact set. Our least-squares-based approach uses novel closed-form approximations of the Pontryagin difference between a constrained zonotopic minuend and a symmetric, convex, and compact subtrahend. We obtain these approximations using two novel canonical representations for full-dimensional constrained zonotopes. Unlike existing approaches, our approach does not rely on convex optimization solvers, and is projection-free for ellipsoidal and zonotopic uncertainty sets. We also propose a least-squares-based approach to compute a convex, polyhedral outer-approximation to constrained zonotopes, and characterize sufficient conditions under which all these approximations are exact. We demonstrate the computational efficiency and scalability of our approach in several case studies, including the design of abort-safe rendezvous trajectories for a spacecraft in near-rectilinear halo orbit under uncertainty. Our approach can inner-approximate a 20-step robust controllable set for a 100-dimensional linear system in under 15 seconds on a standard computer.

Key words: Constrained Zonotopes, Robust controllable set, Computational geometry, Pontryagin difference, Set-based control

1 Introduction

Robust controllable (RC) sets characterize a set of states from which a collection of possibly time-varying state constraints can be satisfied by a controlled state trajectory, under bounded control authority and uncertainty. RC sets are essential for robust model predictive control [1–4], fault-tolerant control [5–8], and verification of dynamical systems [9–12], and have been used in a broad range of applications in space [10–13], transportation [14], and robotics [15, 16]. For discrete-time linear systems with additive uncertainty and bounded, polytopic state and input constraints, exact RC sets are known to be polytopes, and the RC sets may be computed using set computations on polytopes. However, polytope-based RC set computation involves projection that has a combinatorial computational complexity and causes numerical issues for high-dimensional systems and/or over long horizons [3, 16–18]. In this paper, we focus in addressing these shortcomings, and propose *novel theory and algorithms for efficient and scalable computation of inner- and outer-approximations of RC sets, that admit closed-form description of the sets involved and can be computed without relying on convex optimization solvers in several cases.*

We are motivated by the problem of designing *active, abort-safe, spacecraft rendezvous* trajectories with the Lunar gateway [19]. In abort-safe rendezvous, we seek rendezvous trajectories that nominally steer the control-constrained spacecraft towards the rendezvous target, while allowing for the possibility of diverting away from the rendezvous target in the event of failure. Often, failures in space applications are characterized by partial or complete loss of actuation, and increased actuation and navigational uncertainties that may appear as additive uncertainties in the dynamics. For designing such rendezvous trajectories, we use RC sets to characterize a set of state constraints that a nominal trajectory should satisfy, where the RC sets encode the desirable property of safe abort under limited available actuation and uncertainty, similarly to [11, 13]. However, polytope-based computation of RC sets for high-dimensional systems suffers from numerical issues, primarily due to projection [3, 16–18]. On the other hand, our approach can compute the required high-dimensional RC sets.

⋆ This paper was not presented at any IFAC meeting. Corresponding author A. P. Vinod.

Email addresses: vinod@merl.com (Abraham P. Vinod), weiss@merl.com (Avishai Weiss), dicairano@merl.com (Stefano Di Cairano).

We will use constrained zonotopes, a recently proposed alternative description to polytopes [5,6,9,20], to achieve tractable approximation of RC sets. In the disturbance-free setting, constrained zonotopes provide closed-form expressions for all set operations used in the exact computation of the *controllable set* [5]. However, an exact computation of RC sets using constrained zonotopes is hindered by the fact that there are no tractable approaches to compute the exact Pontryagin difference with a constrained zonotopic minuend [6, 9].

Recently, [9] described an optimization-based two-stage approach to inner-approximate the Pontryagin difference between a constrained zonotope and a zonotope, which allows for computing inner-approximations of RC sets when the additive disturbance set is a zonotope. However, it is unclear how such an approach extends to ellipsoidal uncertainty (a more common setting in control), and the reliance of optimization hinders fast computation of RC sets for high-dimensional systems. In this paper, we propose *least-squares-based algorithms to generate constrained zonotopes that inner- and outer-approximate the Pontryagin difference between a constrained zonotopic minuend and a symmetric, convex, and compact subtrahend*. Our approaches also admit closed-form expressions for the approximations when using a full-dimensional minuend, and an ellipsoidal or zonotopic subtrahend. Then, we use these algorithms for fast and scalable computation of RC sets for an additive uncertainty set that is symmetric, convex, and compact.

The main contributions of this paper are as follows: 1) a tractable inner- and outer-approximation of the Pontryagin difference between a constrained zonotopic minuend and a symmetric, convex, and compact subtrahend, 2) an inner- and outer-approximation of the RC sets using the proposed approximations to the Pontryagin difference, 3) a closed-form description of a polyhedral outer-approximation of a constrained zonotope, and 4) sufficient conditions under which the approximations proposed above are exact. We propose two canonical representations for full-dimensional constrained zonotopes, which facilitate the use of the least-squares method as the primary tool for all of our approaches. Efficient implementations for the least-squares method are well-known [21]. Unlike [9], the proposed approximations to the Pontryagin difference admit closed-form expressions when the subtrahend is an ellipsoid, a zonotope, or a convex hull of a collection of symmetric intervals. These features together enable an inner-approximation of a 20-step RC set for a 100-dimensional linear system in less than 15 seconds on a standard computer.

The rest of this paper is organized as follows: Sec. 2 provides the necessary mathematical background and states the problem statements of interest. Sec. 3 and 4 describe the proposed approaches to approximate the Pontryagin difference between a constrained zonotopic minuend and a symmetric, convex, and compact subtrahend. Sec. 5 applies these approaches to the computation of RC sets, and Sec. 6 presents several case studies that demonstrate the utility and scalability of the proposed approach. Sec. 7 applies the method to the (simplified) motivating problem of active abort-safe rendezvous with the Lunar gateway. Sec. 8 summarizes the paper.

2 Preliminaries

$0_{n\times m}$ and $1_{n\times m}$ are matrices of zeros and ones in $\mathbb{R}^{n\times m}$ respectively, I_n is the n-dimensional identity matrix, $\mathbb{N}_{[a:b]}$ is the subset of natural numbers between (and including) $a, b \in \mathbb{N}$, $a \leq b$, $[\![a, b]\!] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$, e_i is the standard axis vectors of $\mathbb{R}^n$, and $\|\cdot\|_p$ is the ℓ_p-norm of a vector. Let M be a matrix and M_1 (M_2, resp.) be another matrix of the same height (width, resp.) as M. Then, $[M, M_1]$ ($[M; M_2]$, resp.) denotes the matrix obtained by concatenating M and M_1 horizontally (concatenating M and M_2 vertically, resp.). For a matrix $M \in \mathbb{R}^{m\times n}$ with full row rank, $M^\dagger = M^\top \left(MM^\top\right)^{-1}$ denotes its (right) pseudoinverse, and $x = M^\dagger v$ solves the system of linear equation $Mx = v$ for any vector $v \in \mathbb{R}^m$ [21, Sec. 11.5]. Given $d \in \mathbb{R}^n$, $\mathrm{diag}(d)$ is a n-dimensional diagonal matrix with diagonal entries d_i.

A set $\mathcal{S} \subset \mathbb{R}^n$ is said to be *symmetric* about any $c \in \mathbb{R}^n$, if $c + x \in \mathcal{S}$ implies $c - x \in \mathcal{S}$ for any $x \in \mathbb{R}^n$. For any set $\mathcal{S} \subseteq \mathbb{R}^n$, we denote its *convex hull* and *affine hull* by $\mathrm{CH}(\mathcal{S})$ and $\mathrm{AH}(\mathcal{S})$ respectively. Recall that $\mathrm{AH}(\mathcal{S})$ is an affine set such that $\mathcal{S} \subseteq \mathcal{A} \Rightarrow \mathrm{AH}(\mathcal{S}) \subseteq \mathcal{A}$ for any affine set $\mathcal{A}$. The *affine dimension* of a set $\mathcal{S}$ is the dimension of the subspace associated with $\mathrm{AH}(\mathcal{S})$. A *full-dimensional* set in $\mathbb{R}^n$ is a non-empty set with an affine dimension of n. See [22, Sec. 2.1] for more details.

2.1 Set representations

Let $\mathcal{C}$ be a convex and compact polytope in $\mathbb{R}^n$. We consider two representations of $\mathcal{C}$ — *H-Rep polytope* (1a) and *constrained zonotope* (1b),

$$\mathcal{C} = \{x \mid H_C x \leq k_C\}, \tag{1a}$$
$$\mathcal{C} = \{G_C\xi + c_C \mid \|\xi\|_\infty \leq 1,\ A_C\xi = b_C\}, \tag{1b}$$

with $H_C \in \mathbb{R}^{L_C\times n}$, $k_C \in \mathbb{R}^{L_C}$, $G_C \in \mathbb{R}^{n\times N_C}$, $c_C \in \mathbb{R}^n$, $A_C \in \mathbb{R}^{M_C\times N_C}$, and $b_C \in \mathbb{R}^{M_C}$. Here, (1a) is the intersection of L_C halfspaces and (1b) is an affine transformation of $\mathcal{B}_\infty(A_C, b_C)$, $\mathcal{C} = c_C + G_C\mathcal{B}_\infty(A_C, b_C)$ with

$$\mathcal{B}_\infty(A_C, b_C) \triangleq \{\xi \mid \|\xi\|_\infty \leq 1, A_C\xi = b_C\}. \tag{2}$$

In (2), $\mathcal{B}_\infty(A_C, b_C)$ is the intersection of a unit-hypercube in $\mathbb{R}^{N_C}$ and M_C linear equalities. By definition, $\mathcal{C} \neq \emptyset$ if and only if $\mathcal{B}_\infty(A_C, b_C) \neq \emptyset$. Other respresentations of $\mathcal{C}$, apart from (1), include vertex representation (V-Rep polytope) [3] and AH-polytopes [23]. We

refer to *unbounded* H-Rep polytopes as *convex polyhedra*, and use $\mathcal{C} = (G_C, c_C, A_C, b_C)$ to denote a polytope $\mathcal{C}$ in constrained zonotope representation (1b).

The equivalence of the representations in (1) was established in [5, Thm. 1]. Additionally, [5, Thm. 1] provides a systematic approach to convert H-Rep polytopes (1a) to constrained zonotopes (1b). However, an exact conversion of (1b) to (1a) is known to be computationally demanding, with existing approaches applicable only for low-dimensional constrained zonotopes [5, Prop. 3].

The representations (1) are not unique. For H-Rep polytopes, a canonical reduction (up to a permutation of rows) is available using linear programming [3,24]. However, no such canonical reduction is available for constrained zonotopes, to the best of our knowledge. On the other hand, several exact and approximate techniques are available to reduce the *representation complexity* of a given constrained zonotope [5,6,25].

Definition 1. (Representation complexity) *[5] Let $\mathscr{O}_C \triangleq (N_C - M_C)/n$ be the* degrees-of-freedom order *of a constrained zonotope $\mathcal{C} = (G_C, c_C, A_C, b_C)$. Then, the representation complexity of $\mathcal{C}$ is $\mathscr{C}(\mathcal{C}) = (M_C, \mathscr{O}_C)$.*

Zonotopes $\mathcal{Z}$, ellipsoids $\mathcal{E}$, and convex unions of symmetric intervals $\mathcal{I}$ are affine transformations of unit balls defined using ℓ_∞-norms, ℓ_2-norms, and ℓ_1-norms respectively. Formally, we define $\mathcal{Z}, \mathcal{E}, \mathcal{I} \subset \mathbb{R}^n$ as follows,

$$\mathcal{Z} \triangleq \{G_Z\xi + c_Z \mid \|\xi\|_\infty \leq 1\}, \tag{3a}$$
$$\mathcal{E} \triangleq \{G_E\xi + c_E \mid \|\xi\|_2 \leq 1\}, \tag{3b}$$
$$\mathcal{I} \triangleq \{G_I\xi + c_I \mid \|\xi\|_1 \leq 1\}, \tag{3c}$$

with $G_Z \in \mathbb{R}^{n\times N_Z}$, $G_E \in \mathbb{R}^{n\times n}$, $G_I \in \mathbb{R}^{n\times N_I}$, and $c_Z, c_E, c_I \in \mathbb{R}^n$. The sets $\mathcal{Z}, \mathcal{E}, \mathcal{I}$ are symmetric about c_Z, c_E, c_I. We denote these sets using (G, c).

For a convex and compact set $\mathcal{S} \subset \mathbb{R}^n$, its support function $\rho : \mathbb{R}^n \to \mathbb{R}$ and support vector $\vartheta : \mathbb{R}^n \to \mathbb{R}^n$ are

$$\vartheta_{\mathcal{S}}(\nu) \triangleq \arg\sup_{s\in\mathcal{S}} \ \nu^\top s, \text{ and } \rho_{\mathcal{S}}(\nu) \triangleq \nu^\top \vartheta_{\mathcal{S}}(\nu). \tag{4}$$

Using *dual norms* [22, Sec. A.1.6] and properties of support function [26, Prop. 2], we have closed-form expressions for the support function of zonotopes $\mathcal{Z}$, ellipsoids $\mathcal{E}$, and convex unions of symmetric intervals $\mathcal{I}$,

$$\rho_{\mathcal{I}}(\nu) = \nu^\top c_I + \|G_I^\top \nu\|_\infty, \tag{5a}$$
$$\rho_{\mathcal{E}}(\nu) = \nu^\top c_E + \|G_E^\top \nu\|_2, \tag{5b}$$
$$\rho_{\mathcal{Z}}(\nu) = \nu^\top c_Z + \|G_Z^\top \nu\|_1. \tag{5c}$$

2.2 Set operations

For any sets $\mathcal{C}, \mathcal{S} \subseteq \mathbb{R}^n$ and $\mathcal{W} \subseteq \mathbb{R}^m$, and a matrix $R \in \mathbb{R}^{m\times n}$, we define the set operations (affine map, Minkowski sum $\oplus$, intersection with inverse affine map $\cap_R$, and Pontryagin difference $\ominus$):

$$R\mathcal{C} \triangleq \{Ru \mid u \in \mathcal{C}\}, \tag{6a}$$
$$\mathcal{C} \oplus \mathcal{S} \triangleq \{u + v \mid u \in \mathcal{C},\ v \in \mathcal{S}\}, \tag{6b}$$
$$\mathcal{C} \cap_R \mathcal{W} \triangleq \{u \in \mathcal{C} \mid Ru \in \mathcal{W}\}, \tag{6c}$$
$$\mathcal{C} \ominus \mathcal{S} \triangleq \{u \mid \forall v \in \mathcal{S}, u + v \in \mathcal{C}\}. \tag{6d}$$

Since $\mathcal{C} \cap \mathcal{S} = \mathcal{C} \cap_{I_n} \mathcal{S}$, (6c) also includes the standard intersection. For any $x \in \mathbb{R}^n$, we use $\mathcal{C} + x$ and $\mathcal{C} - x$ to denote $\mathcal{C} \oplus \{x\}$ and $\mathcal{C} \oplus \{-x\}$ respectively for brevity.

Constrained zonotopes admit closed-form expressions for various set operations described in (6). From [5,6],

$$R\mathcal{C} = (RG_C, Rc_C, A_C, b_C), \tag{7a}$$
$$\mathcal{C} \oplus \mathcal{S} = ([G_C, G_S], c_C + c_S, [A_C, 0; 0, A_S], [b_C; b_S]), \tag{7b}$$
$$\mathcal{C} \cap_R \mathcal{W} = ([G_C, 0], c_C, [A_C, 0; 0, A_W; RG_C, -G_W], [b_C; b_W; c_W - Rc_C]), \tag{7c}$$
$$\mathcal{C} \cap \mathcal{H} = \big([G_C, 0], c_C, [A_C, 0; p^\top G_C, d_m/2], [b_C; (q + p^\top c_C - \|p^\top G_C\|_1)/2]\big), \tag{7d}$$

where $\mathcal{H} = \{x \mid p^\top x \leq q\} \subset \mathbb{R}^n$ is an halfspace, and (7d) also enables an exact computation of the intersection of a constrained zonotope and a convex polyhedron.

To the best of our knowledge, the Pontryagin difference (6d) involving a constrained zonotopic minuend does not have a closed-form expression, similar to (7) [6, 9]. In fact, given a constrained zonotope $\mathcal{C}$ and a zonotope $\mathcal{Z}$, it is impossible to find a polynomial-size constrained zonotope $\mathcal{C} \ominus \mathcal{Z}$ in polynomial-time, unless P=NP [9, Prop. 1]. On the other hand, given a H-Rep polytope $\mathcal{P} = \{x \mid H_P x \leq k_P\}$ and a convex and compact subtrahend $\mathcal{S}$, a H-Rep polytope $\mathcal{P} \ominus \mathcal{S}$ is available in closed-form,

$$\mathcal{P} \ominus \mathcal{S} = \{x \mid H_P x \leq k_P - [\rho_{\mathcal{S}}(h_1);\ \ldots; \rho_{\mathcal{S}}(h_{L_P})]\}, \tag{8}$$

with $H_P = [h_1^\top; h_2^\top; \ldots; h_{L_C}^\top]$ [27, Thm. 2.3]. A direct use of (8) to compute a constrained zonotope $\mathcal{C} \ominus \mathcal{S}$ for a constrained zonotope minuend $\mathcal{C}$ is prevented by the difficulty in converting (1b) to (1a).

Recently, [9] proposed a two-stage approach to inner-approximate $\mathcal{C} \ominus \mathcal{S}$ between a constrained zonotopic minuend $\mathcal{C}$ and a zonotopic subtrahend $\mathcal{S}$ with $G_S = \left[g_S^{(1)}, \ldots, g_S^{(N_S)}\right]$. The two-stage approach first solves a linear program with $2N_C N_S$ variables,

$$\begin{aligned} \text{minimize} \quad & \text{SumAbs}(\Gamma) \\ \text{s. t.} \quad & [G_C; A_C]\Gamma = [G_S; 0_{M_C\times N_S}], \\ \forall i \in \mathbb{N}_{[1:N_C]}, \quad & \textstyle\sum_{j=1}^{N_S} |\Gamma_{ij}| \leq 1, \end{aligned} \tag{9}$$

where $\text{SumAbs}(\Gamma) \triangleq \sum_{i=1}^{N_C}\sum_{j=1}^{N_S}|\Gamma_{ij}|$. Let the optimal solution to (9) be Γ^*, if it exists, and the second stage defines a diagonal matrix $D \in \mathbb{R}^{N_C \times N_C}$ with

$$D_{ii} = 1 - \|e_i^\top \Gamma^*\|_1 = 1 - \sum_{j=1}^{N_S} |\Gamma^*_{ij}| \tag{10}$$

for each $i \in \mathbb{N}_{[1:N_C]}$. Then, a constrained zonotopic inner-approximation of $\mathcal{C} \ominus \mathcal{S}$ is

$$\mathcal{M}^- \triangleq (G_C D, c_C - c_S, A_C D, b_C) \subseteq \mathcal{C} \ominus \mathcal{S}. \tag{11}$$

Here, $\mathscr{C}(\mathcal{M}^-) = \mathscr{C}(\mathcal{C})$, which is desirable when using (11) in set recursions involving the Pontryagin difference. However, solving (9) repeatedly can become computationally expensive for large N_C, N_S. Also, it is unclear if such an approach extends to subtrahends beyond zonotopes, since it uses polytopic containment results from [23]. We address these shortcomings in this paper.

Problem 1. *Let $\mathcal{C}$ be a constrained zonotope and $\mathcal{S}$ be a convex and compact set that is symmetric about $c_S \in \mathbb{R}^n$. Characterize constrained zonotopes $\mathcal{M}^-, \mathcal{M}^+ \subset \mathbb{R}^n$ with*

$$\mathcal{M}^- \subseteq \mathcal{M} \triangleq \mathcal{C} \ominus \mathcal{S} \subseteq \mathcal{M}^+, \tag{12}$$

where $\mathcal{M}^-$ is given in closed-form and $\mathscr{C}(\mathcal{M}^-) = \mathscr{C}(\mathcal{C})$. Also, provide sufficient conditions for $\mathcal{M}^- = \mathcal{M} = \mathcal{M}^+$.

Our approach to address Prob. 1 follows a similar two-stage approach to that in [9] to obtain (11). However, unlike [9], we provide closed-form expressions for Γ and D used in (10) and (11) for a broader class of subtrahends that includes ellipsoids and convex unions of symmetric intervals. We also propose a constrained zonotopic outer-approximation to $\mathcal{M}$, and provide sufficient conditions under which these approximations are exact. The proposed outer-approximation relies on solving the following problem.

Problem 2. *Given a constrained zonotope $\mathcal{C}$, design an algorithm to compute an outer-approximating convex polyhedron $\mathcal{P}$ (i.e, $\mathcal{P} \supseteq \mathcal{C}$) in the form of* (1a) *that has at most $2N_C$ linear constraints. Also, provide sufficient conditions under which $\mathcal{C} = \mathcal{P}$.*

We will also briefly discuss the relationship between the proposed approach and the two-stage approach in [9].

2.3 Robust controllable set

Consider a linear time-varying system,

$$x_{t+1} = A_t x_t + B_t u_t + F_t w_t, \tag{13}$$

with state $x_t \in \mathbb{R}^n$, input $u_t \in \mathcal{U}_t \subset \mathbb{R}^m$, disturbance $w_t \in \mathcal{W}_t \subset \mathbb{R}^p$, and appropriately defined time-varying matrices A_t, B_t, and F_t.

Definition 2. (T-Step RC set) *[3, Defn. 10.18] Given* (13)*, a set of (possibly time-varying) state constraints $\{\mathcal{X}_t\}_{t=0}^{T-1}$ with $\mathcal{X}_t \subseteq \mathbb{R}^n$ for each t, and a goal set $\mathcal{G} \subset \mathbb{R}^n$, the T-step robust controllable (RC) set is*

$$\mathcal{K} = \left\{ x_0 \in \mathcal{X}_0 \;\middle|\; \begin{array}{c} \forall t \in \mathbb{N}_{[0:T-1]},\ \exists u_t \in \mathcal{U}_t,\ \forall w_t \in \mathcal{W}_t, \\ x_{t+1} = A_t x_t + B_t u_t + F_t w_t, \\ x_t \in \mathcal{X}_t,\ x_T \in \mathcal{G} \end{array} \right\}.$$

Informally, the T-step RC set $\mathcal{K} \subset \mathbb{R}^n$ is the set of initial states that, despite the additive disturbance $w_t \in \mathcal{W}_t$, can be steered using $u_t \in \mathcal{U}_t$ to reach the goal set $\mathcal{G}$ at time step T, while staying within the state constraints $\mathcal{X}_t$ at all intermediate time steps $t \in \mathbb{N}_{[0:T-1]}$. The T-step RC set is also known as robust reachability of target tube [4], backward reachable set [9], or backward reach-avoid set [10]. The following set recursion yields $\mathcal{K} = \mathcal{K}_0$,

$$\mathcal{K}_t = \text{Pre}(\mathcal{K}_{t+1}) \cap \mathcal{X}_t, \qquad \forall t \in \mathbb{N}_{[0:T-1]}, \tag{14a}$$

$$\text{Pre}(\mathcal{K}_{t+1}) \triangleq \{x \mid A_t x \in (\mathcal{K}_{t+1} \ominus F_t \mathcal{W}_t) \oplus (-B_t \mathcal{U}_t)\}, \tag{14b}$$

with $\mathcal{K}_T \triangleq \mathcal{G}$. Observe that (14) uses all set operations in (6). For H-Rep/V-Rep polytopes $\mathcal{X}, \mathcal{G}, \mathcal{U}$, and $\mathcal{W}$, we can compute RC sets using existing results [3, 10, 24]. However, when using H-Rep/V-Rep polytopes for high-dimensional systems (13) or over long horizons T, we face numerical challenges when implementing (14), since it requires a combination of Minkowski sum and intersection operations. See [3, 16–18] for a detailed discussion.

On the other hand, constrained zonotopes provide a tractable, exact solution when $\mathcal{W} = \emptyset$ using (7) [5, 6, 9]. Also, for a zonotopic $\mathcal{W}$, [9] uses the two-stage approach reviewed in Sec. 2.2 to propose an inner-approximation of $\mathcal{K}$. In this paper, we use our solution to Prob. 1 to inner-approximate $\mathcal{K}$ for a broader class of sets $\mathcal{W}$.

Problem 3. *Compute a constrained zonotope $\mathcal{K}^-$ that inner-approximates $\mathcal{K}$ defined in Defn. 2, where for every $t \in \mathbb{N}_{[0:T-1]}$, $\mathcal{U}_t$ and $\mathcal{G}$ are polytopes, $\mathcal{W}_t$ are symmetric, convex, and compact sets, and either 1) $\mathcal{X}_t$ are convex polyhedra and A_t are invertible, or 2) $\mathcal{X}_t$ are polytopes. Additionally, characterize the representation complexity of $\mathcal{K}^-$ in both cases.*

In both settings considered, the exact RC sets are known to be polytopes [3], and hence are representable via constrained zonotopes. We also use the proposed outer-approximation to the Pontryagin difference to outer-approximate $\mathcal{K}_t$ when using (14).

3 Inner-approximation of Pontryagin difference

Given a constrained zonotopic minuend $\mathcal{C} \subset \mathbb{R}^n$ and a symmetric, convex, and compact subtrahend $\mathcal{S} \subset \mathbb{R}^n$,

Subtrahend $\mathcal{S}$	Definition of the diagonal matrix $D = \text{diag}_{i\in\mathbb{N}_{[1:N_C]}}(D_{ii})$	Result
Convex and compact $\mathcal{S}$, symmetric about $c_S \in \mathbb{R}^n$	$D_{ii} = 1 - \rho_{\mathcal{S}_0}\left(e_i^\top [G_C; A_C]^\dagger [I_n; 0_{M_C\times n}]\right)$ for $\mathcal{S}_0 \triangleq \mathcal{S} - c_S$	Prop. 2
Zonotope $\mathcal{S}$ (3a)	$D_{ii} = 1 - \left\|e_i^\top [G_C; A_C]^\dagger [G_S; 0_{M_C\times N_S}]\right\|_1$	Corr. 1
Ellipsoid $\mathcal{S}$ (3b)	$D_{ii} = 1 - \left\|e_i^\top [G_C; A_C]^\dagger [G_S; 0_{M_C\times n}]\right\|_2$	
Convex union of symmetric intervals $\mathcal{S}$ (3c)	$D_{ii} = 1 - \left\|e_i^\top [G_C; A_C]^\dagger [G_S; 0_{M_C\times N_S}]\right\|_\infty$	

Table 1
Summary of the closed-form expressions for the diagonal matrix $D = \text{diag}_{i\in\mathbb{N}_{[1:N_C]}}(D_{ii})$ for various subtrahends $\mathcal{S}$ that is symmetric about $c_S \in \mathbb{R}^n$, and the corresponding result in the paper. Given a full-dimensional constrained zonotopic minuend $\mathcal{C} = (G_C, c_C, A_C, b_C)$, we propose a constrained zonotope $\mathcal{M}^- = (G_C D, c_C - c_S, A_C D, b_C)$ that satisfies $\mathcal{M}^- \subseteq \mathcal{M} = \mathcal{C} \ominus \mathcal{S}$.

Algorithm 1 Compute MinRow representation

Input: Constrained zonotope (G_C, c_C, A_C, b_C) that represents a full-dimensional polytope
Output: MinRow representation (G'_C, c'_C, A'_C, b'_C)
1: Set $G'_C \leftarrow G_C$ and $c'_C \leftarrow c_C$.
2: Get A'_C, b'_C from rows of $[A_C, b_C]$ where $[A'_C, b'_C]$ has full row rank and $\text{rank}([A'_C, b'_C]) = \text{rank}([A_C, b_C])$.

we characterize a constrained zonotope $\mathcal{M}^- \subset \mathbb{R}^n$ where

$$\mathcal{M}^- \subseteq \mathcal{M} \triangleq \mathcal{C} \ominus \mathcal{S}. \tag{15}$$

Specifically, we provide closed-form expressions for a diagonal matrix $D \in \mathbb{R}^{N_C\times N_C}$ using the properties of $\mathcal{C}$ and $\mathcal{S}$, and define $\mathcal{M}^- = (G_{M^-}, c_{M^-}, A_{M^-}, b_{M^-})$ with

$$G_{M^-} = G_C D, \qquad c_{M^-} = c_C - c_S, \tag{16a}$$
$$A_{M^-} = A_C D, \qquad b_{M^-} = b_C, \tag{16b}$$

for a specific $c_S \in \mathcal{S}$, similarly to (11). The representation complexity of $\mathcal{M}^-$ is $\mathscr{C}(\mathcal{M}^-) = (M_C, \mathscr{O}_C) = \mathscr{C}(\mathcal{C})$.

In this section, we propose two constrained zonotope representations that allow us to address Prob. 1, and relate our approach with the two-stage approach in [9] for zonotopic subtrahends. Table 1 summarizes the computation of D for various types of sets.

3.1 Full-dimensional constrained zonotopes

We study two constrained zonotope representations that are guaranteed to exist for full-dimensional polytopes.

Definition 3. (MinRow Representation) *A constrained zonotope $\mathcal{C} = (G_C, c_C, A_C, b_C)$ is a* MinRow *representation when $[G_C; A_C]$ has full row rank.*

Definition 4. (Invertible representation) *A* MinRow *representation $\mathcal{C}$ is an* Invertible *representation when $n + M_C = N_C$, i.e., $\mathscr{O}_\mathcal{C} = 1$.*

By definitions, the matrix $[G_C; A_C] \in \mathbb{R}^{(n+M_C)\times N_C}$ has a well-defined right pseudoinverse $[G_C; A_C]^\dagger$ for a MinRow representation, and $[G_C; A_C]$ is invertible for an Invertible representation. Fig. 1 illustrates the relationships between the representations based on Prop. 1.

Algorithm 2 Compute Invertible representation

Input: H-Rep polytope $\mathcal{C} = \{x \mid H_C x \le k_C\} \subset \mathbb{R}^n$ that represents a full-dimensional polytope
Output: Invertible representation (G_C, c_C, A_C, b_C)
1: Define a zonotope $\mathcal{Z} = (G_Z, c_Z)$ (3a) with $G_Z \triangleq \text{diag}\left(\frac{u-l}{2}\right) \in \mathbb{R}^{n\times n}$, $c_Z \triangleq \frac{u+l}{2} \in \mathbb{R}^n$ for $l, u \in \mathbb{R}^n$,
$$l_i = -\rho_\mathcal{C}(-e_i), \quad u_i = \rho_\mathcal{C}(e_i), \quad \forall i \in \mathbb{N}_{[1:n]}. \tag{17}$$
2: Define $\sigma \in \mathbb{R}^{L_C}$ with $\sigma_i = -\rho_\mathcal{Z}(-h_i)$ for each $i \in \mathbb{N}_{[1:L_C]}$ and $H_C = [h_1^\top; h_2^\top; \ldots; h_{L_C}^\top]$.
3: Compute the Invertible representation for $\mathcal{C}$ with
$$G_C = [G_Z, 0_{n\times L_C}], \qquad c_C = c_Z,$$
$$A_C = \left[H_C G_Z, \text{diag}\left(\frac{\sigma - k}{2}\right)\right], \quad b_C = \frac{\sigma + k}{2} - H_C c_Z.$$

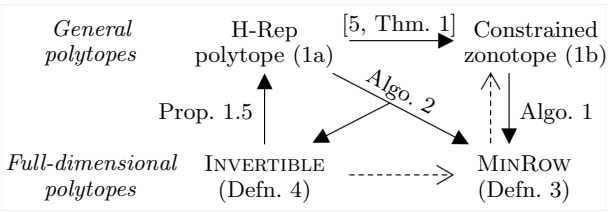

Fig. 1. Relationship between various representations discussed in the paper. For any pair of representations R_1, R_2, a dashed arrow from R_1 to R_2 shows that R_1 is also R_2.

Proposition 1. *The following statements hold:*
1) Every representation (G_C, c_C, A_C, b_C) of a full-dimensional polytope $\mathcal{C}$ satisfies $\text{rank}(G_C) = n \le N_C$.
2) A polytope is full-dimensional if and only if the polytope is non-empty and it has a MinRow *representation.*
3) Algo. 1 generates a MinRow *representation from any full-dimensional constrained zonotope* (1b).
4) Algo. 2 generates an Invertible *representation from any full-dimensional H-Rep polytope* (1a).
5) Given an Invertible *representation (G_C, c_C, A_C, b_C), the corresponding H-Rep polytope* (1a) *is given by,*

$$H_C = [I_{N_C}; -I_{N_C}]\,[G_C; A_C]^{-1}\,[I_n; 0_{M_C\times n}]\,, \tag{18a}$$
$$k_C = 1_{2N_C\times 1} - [I_{N_C}; -I_{N_C}]\,[G_C; A_C]^{-1}\,[-c; b]\,. \tag{18b}$$

See Sec. A.1 for the proof of Prop. 1. Step 2 in Algo. 1 removes redundant equalities in $\{\xi \mid A_C\xi = b_C\}$. See `mpt_minAffineRep` in MPT3 [24] for an implementation.

By Prop. 1.4, an Invertible representation also exists

for every full-dimensional constrained zonotope. However, it is unclear if we can efficiently compute such a representation from an arbitrary full-dimensional constrained zonotope, as done in Algo. 1.

Remark 1. *The rest of the paper assumes the use of a* MinRow *representation for any full-dimensional constrained zonotope, obtained using either Algo. 1 or 2.*

3.2 Inner-approximation of the Pontryagin difference

Thm. 1 tackles the inner-approximation part of Prob. 1.

Theorem 1. *Given a non-empty constrained zonotopic minuend $\mathcal{C} = (G_C, c_C, A_C, b_C) \subset \mathbb{R}^n$ and a convex and compact subtrahend $\mathcal{S} \subset \mathbb{R}^n$ that is symmetric about any $c_S \in \mathbb{R}^n$. Let $\Gamma : \mathbb{R}^{N_C \times n}$ solve*

$$[G_C; A_C]\Gamma = [I_n; 0_{M_C \times n}], \tag{19}$$

and $D \in \mathbb{R}^{N_C \times N_C}$ be a diagonal matrix with

$$D_{ii} \triangleq 1 - \rho_{\mathcal{S}_0}\left(e_i^\top \Gamma\right), \tag{20}$$

for each $i \in \mathbb{N}_{[1:N_C]}$, where $\mathcal{S}_0 \triangleq \mathcal{S} - c_S$. Then, the constrained zonotope $\mathcal{M}^-$ defined using (16) and D in (20) satisfies (15), provided $D_{ii} \geq 0$ for every $i \in \mathbb{N}_{[1:N_C]}$.

Proof. Given $\mathcal{S}_0 \subset \mathbb{R}^n$, define $\mathcal{V}_0 = \Gamma\mathcal{S}_0 \subset \mathbb{R}^{N_C}$. By definition of Γ, $\mathcal{V}_0$ satisfies 1) $G_C\mathcal{V}_0 = \mathcal{S}_0 = \mathcal{S} - c_S$, and 2) $A_C\mathcal{V}_0 = \{0_{M_C \times 1}\}$.

Next, define $\mathcal{C}_L \triangleq \mathcal{B}_\infty(A_C, b_C) \ominus \mathcal{V}_0 \subset \mathbb{R}^{N_C}$, and define

$$\mathcal{M}^- \triangleq c_{M^-} + G_C\mathcal{C}_L. \tag{21}$$

with c_{M^-} in (16). Recall that for any set $\mathcal{A}, \mathcal{B} \subset \mathbb{R}^n$ and a matrix $M \in \mathbb{R}^{m \times n}$ with $m < n$, $M(\mathcal{A} \ominus \mathcal{B}) \subseteq (M\mathcal{A}) \ominus (M\mathcal{B})$ [9, Lem. 2(ii)]. From [27, Thm. 2.1.iv],

$$\begin{aligned}\mathcal{M}^- &\subseteq c_{M^-} + (G_C\mathcal{B}_\infty(A_C, b_C) \ominus (G_C\mathcal{V}_0))\\ &= c_{M^-} + ((\mathcal{C} - c_C) \ominus (\mathcal{S} - c_S))\\ &= (c_{M^-} - (c_C - c_S)) + (\mathcal{C} \ominus \mathcal{S}) = \mathcal{C} \ominus \mathcal{S}. \end{aligned} \tag{22}$$

Next, we simplify $\mathcal{C}_L$ as follows,

$$\begin{aligned}\mathcal{C}_L &= \{\xi \mid \forall v \in \mathcal{V}_0,\ \xi + v \in \mathcal{B}_\infty(A_C, b_C)\} && (23)\\ &= \{\xi \mid \forall v \in \mathcal{V}_0,\ A_C(\xi + v) = b_C,\ \|\xi + v\|_\infty \leq 1\} && (24)\\ &= \{\xi \mid A_C\xi = b_C,\ \forall v \in \mathcal{V}_0,\ \|\xi + v\|_\infty \leq 1\} && (25)\\ &= \{\xi \mid A_C\xi = b_C\} \cap \left(\{\xi \mid \|\xi\|_\infty \leq 1\} \ominus \mathcal{V}_0\right) && (26)\\ &= \left\{\xi \;\middle|\; \begin{array}{c} A_C\xi = b_C,\ \forall i \in \mathbb{N}_{[1:N_C]},\ \forall \delta \in \{-1, 1\},\\ \delta e_i^\top \xi \leq 1 - \rho_{\mathcal{V}_0}(\delta e_i)\end{array}\right\} && (27)\\ &= \left\{\xi \;\middle|\; \begin{array}{c} A_C\xi = b_C,\ \forall i \in \mathbb{N}_{[1:N_C]},\\ |e_i^\top \xi| \leq 1 - \rho_{\mathcal{S}_0}\left(\Gamma^\top e_i\right)\end{array}\right\} && (28)\\ &= \left\{\xi \;\middle|\; A_C\xi = b_C,\ \forall i \in \mathbb{N}_{[1:N_C]},\ \left|e_i^\top \xi\right| \leq D_{ii}\right\}. && (29)\end{aligned}$$

Here, (23) follows from (6d) and the definition of $\mathcal{C}_L$, (24) follows from (2), (25) follows from the choice of $\mathcal{V}_0$, (26) follows from (6d), (27) follows from (8), (28) follows from (4) and from $\rho_{\mathcal{V}_0}(\nu) = \rho_{\mathcal{S}_0}(\Gamma^\top \nu)$ for all $\nu \in \mathbb{R}^{N_C}$ [26, Prop. 2], and from symmetry of $\mathcal{S}_0$ about the origin implying $\rho_{\mathcal{S}_0}(-\mu) = \rho_{\mathcal{S}_0}(\mu)$ for all $\mu \in \mathbb{R}^n$ by (4), and (29) follows from the definition of D_{ii} (20).

If $D_{ii} < 0$ for any $i \in \mathbb{N}_{[1:N_C]}$, then $\mathcal{C}_L = \emptyset$ by (29), and $\mathcal{M}^-$ defined in (21) is also empty. On the other hand, when $D_{ii} \geq 0$ for all $i \in \mathbb{N}_{[1:N_C]}$, (29) may be expressed as a scaled version of $\mathcal{B}_\infty$,

$$\mathcal{C}_L = \{D\xi \mid A_C D\xi = b_C,\ \|\xi\|_\infty \leq 1\} = D\mathcal{B}_\infty(A_C D, b_C).$$

Thus, $\mathcal{M}^- \subseteq \mathcal{C} \ominus \mathcal{S}$ in (15) using (21) and (22), provided $D_{ii} \geq 0$ for all $i \in \mathbb{N}_{[1:N_C]}$. □

Thm. 1 inner-approximates the Pontryagin difference (6d) using the support function of the subtrahend $\mathcal{S}$. The condition $D_{ii} \geq 0$ for all $i \in \mathbb{N}_{[1:N_C]}$ in Thm. 1 may be viewed as requiring Γ to additionally satisfy $\Gamma\mathcal{S}_0 \subseteq \{\xi \mid \|\xi\|_\infty \leq 1\}$. Such a choice ensures $\rho_{\mathcal{S}_0}\left(\Gamma^\top e_i\right) \leq 1$, and thereby, $D_{ii} \geq 0$ [22, Ex. 3.35(d)].

Proposition 2. *For a full-dimensional, constrained zonotopic minuend $\mathcal{C}$ and a convex and compact subtrahend $\mathcal{S} \subset \mathbb{R}^n$ that is symmetric about any $c_S \in \mathbb{R}^n$, the constrained zonotope $\mathcal{M}^-$ defined in Thm. 1 with $\Gamma = [G_C; A_C]^\dagger [I_n; 0_{M_C \times n}]$ inner-approximates $\mathcal{C} \ominus \mathcal{S}$.*

Proof. Follows from Rem. 1 and Thm. 1. □

Prop. 2 addresses Prob. 1. Additionally, we use the following two observations to illustrate that the assumption of full-dimensionality in Prop. 2 is not restrictive. First, $\mathcal{C} \ominus \mathcal{S} = \emptyset$, whenever the affine dimension of $\mathcal{S}$ is strictly greater than the affine dimension of $\mathcal{C}$ by (6d), since $x + \mathcal{S}$ can not be contained in $\mathcal{C}$ for any $x \in \mathbb{R}^n$ in such a scenario. Second, consider the case where both minuend and subtrahend are not full-dimensional and there exists a matrix $T \in \mathbb{R}^{n \times n'}$ with $n > n'$ and $\operatorname{rank}(T) = n'$ such that $\mathcal{C} = T\mathcal{C}'$ and $\mathcal{S} = T\mathcal{S}'$ for any $\mathcal{C}', \mathcal{S}' \subset \mathbb{R}^{n'}$. Then, by [27, Thm. 2.1.viii],

$$\mathcal{C} \ominus \mathcal{S} = (T\mathcal{C}') \ominus (T\mathcal{S}') = T(\mathcal{C}' \ominus \mathcal{S}'). \tag{30}$$

In such a case, it suffices to assume that $\mathcal{C}'$ is full-dimensional in order to obtain a constrained zonotope inner-approximation of $\mathcal{C} \ominus \mathcal{S}$.

Corollary 1 (Special cases)**.** *For a full-dimensional constrained zonotopic minuend $\mathcal{C}$, D in (20) has closed-form expressions for D_{ii} for each $i \in \mathbb{N}_{[1:N_C]}$:*
1) when $\mathcal{S}$ is a zonotope (3a),

$$D_{ii} = 1 - \left\|e_i^\top [G_C; A_C]^\dagger [G_S; 0_{M_C \times N_S}]\right\|_1, \tag{31}$$

Algorithm 3 Inner-approximation of $\mathcal{C} \ominus \mathcal{S}$

Input: Minuend $\mathcal{C} = (G_C, c_C, A_C, b_C)$ that is full-dimensional and subtrahend $\mathcal{S}$ that is convex, compact, and symmetric about any $c_S \in \mathbb{R}^n$
Output: Constrained zonotope $\mathcal{M}^- \subseteq \mathcal{C} \ominus \mathcal{S}$
1: $\mathcal{S}_0 \leftarrow \mathcal{S} - c_S$
2: $\Gamma \leftarrow [G_C; A_C]^\dagger [I_n; 0_{M_C \times n}]$
3: $D \leftarrow \operatorname{diag}([1 - \rho_{\mathcal{S}_0}(e_1^\top \Gamma); \ldots; 1 - \rho_{\mathcal{S}_0}(e_{N_C}^\top \Gamma)])$
4: $\mathcal{M}^- \leftarrow \begin{cases} (G_C D, c_C - c_S, A_C D, b_C), & \min\limits_{i \in \mathbb{N}_{[1:N_C]}} D_{ii} \geq 0, \\ \emptyset, & \text{otherwise} \end{cases}$.

2) when $\mathcal{S}$ is an ellipsoid (3b),

$$D_{ii} = 1 - \left\| e_i^\top [G_C; A_C]^\dagger [G_S; 0_{M_C \times N_S}] \right\|_2, \tag{32}$$

3) when $\mathcal{S}$ is a convex union of symmetric intervals (3c),

$$D_{ii} = 1 - \left\| e_i^\top [G_C; A_C]^\dagger [G_S; 0_{M_C \times N_S}] \right\|_\infty. \tag{33}$$

Proof. Follows from (5) and Prop. 2. □

Corr. 1 lists some broad classes of subtrahends that admits closed-form expressions for the inner-approximation $\mathcal{M}^-$ of the Pontryagin difference $\mathcal{C} \ominus \mathcal{S}$.

Algo. 3 summarizes the procedure described in Prop. 2 to inner-approximate $\mathcal{C} \ominus \mathcal{S}$ when the minuend $\mathcal{C}$ is full-dimensional. For subtrahends that are ellipsoids, zonotopes, or convex unions of symmetric intervals, Step 3 in Algo. 3 is available in closed form (see Corr. 1), and Algo. 3 is optimization-free, i.e., it does not require convex optimization solvers.

Remark 2. *We can also use a "template" constrained zonotope $\mathcal{C}^- \subseteq \mathcal{C}$ when available and compute $\mathcal{C}^- \ominus \mathcal{S} \subseteq \mathcal{C} \ominus \mathcal{S}$ using Thm. 1. Such an approach may help in overcoming conservativeness in certain cases, e.g., $\mathcal{M}^-$ described in Thm. 1 is a zonotope for zonotopes $\mathcal{C}, \mathcal{S}$, even when $\mathcal{C} \ominus \mathcal{S}$ is known to be a constrained zonotope [6, 9].*

3.3 Relation of Algo. 3 with existing two-stage approach for zonotopic subtrahend

For a zonotopic subtrahend $\mathcal{S}$, the optimization-free Algo. 3 is closely related to the optimization-based two-stage approach [9] (see Sec. 2.2).

Let $\mathcal{S} = G_S \mathcal{S}_0 + c_S$ where $\mathcal{S}_0$ is the unit ℓ_∞-norm ball (3a). Consider the *matrix least norm* problem [21, Ex. 16.2], which is similar to (9) where the objective is now the Frobenius norm $\|\Gamma\|_F \triangleq \sqrt{\sum_{i=1}^{N_C} \sum_{j=1}^{N_S} \Gamma_{ij}^2}$,

$$\begin{aligned} \underset{\Gamma \in \mathbb{R}^{N_C \times N_S}}{\text{minimize}} \quad & \|\Gamma\|_F \\ \text{subject to} \quad & [G_C; A_C]\Gamma = [G_S; 0_{M_C \times N_S}]. \end{aligned} \tag{34}$$

Algorithm 4 Convex polyhedral outer-approximation of a constrained zonotope $\mathcal{C}$

Input: Full-dimensional $\mathcal{C} = (G_C, c_C, A_C, b_C)$
Output: Convex polyhedron $\mathcal{P} = \{x \mid Hx \leq k\} \supseteq \mathcal{C}$
1: $V \leftarrow [v_1; v_2; \ldots; v_{N_C}] \in \mathbb{R}^{N_C \times (n + M_C)}$ with

$$v_i = \frac{e_i^\top [G_C; A_C]^\dagger}{\left\| e_i^\top [G_C; A_C]^\dagger [G_C; A_C] \right\|_1}, \ \forall i \in \mathbb{N}_{[1:N_C]} \tag{35}$$

2: $H \leftarrow [V; -V][I_n; 0_{M_C \times n}]$
3: $k \leftarrow 1_{2N_C \times 1} - [V; -V][-c_C; b_C]$

When $\mathcal{C}$ is full-dimensional, the optimal solution of (34) is available in closed-form, $\Gamma^* = [G_C; A_C]^\dagger [G_S; 0_{M_C \times N_S}]$, by Prop. 1.2 and [21, Ex. 16.2]. Observe that $\Gamma^* = \Gamma G_S$ for Γ prescribed by Prop. 2. Then, we can recover D prescribed by (31) in Corr. 1 using (20) in Thm. 1, where $\rho_{\mathcal{S}_0}(\nu) = \|\nu\|_1$ instead of (5c).

The condition $D_{ii} \geq 0$ for every $i \in \mathbb{N}_{[1:N_C]}$ is required in the two-stage approach [9] (see (9)) and in Step 4 of Algo. 3. Thus, Algo. 3 and [9] differ only in the choice of Γ (or specifically, the choice of objective in (9)) for a zonotopic subtrahend. In other words, Algo. 3 may be viewed as a generalization of [9] for symmetric, convex, and compact subtrahends, and does not require an optimization solver for certain subtrahends (Corr. 1). We compare these approaches in various examples in Sec. 6.

4 Outer-approximation of Pontryagin difference and sufficient conditions for exactness

In this section, we first address Prob. 2, and then use its solution to address the outer-approximation part of Prob. 1. We also provide sufficient conditions under which all proposed approximations are exact. We conclude this section with a discussion of implementation considerations for the proposed algorithms.

4.1 Outer-approximating convex polyhedron for a given constrained zonotope

We now address Prob. 2 using Algo. 4.

Proposition 3. *Given a full-dimensional constrained zonotope $\mathcal{C}$, Algo. 4 computes a convex, polyhedral, outer-approximation of $\mathcal{C}$ with at most $2N_C$ linear constraints.*

See Sec. A.2 for the proof. We used the observation that a full-dimensional $\mathcal{C}$ may be expressed as the 1-sublevel set of the optimal value function of a feasible linear program. Using strong duality, we obtain an outer-approximating convex polyhedron $\mathcal{P}$, characterized by $2N_C$ feasible solutions (35) to the corresponding dual problem.

While [5, Prop. 3] provides an exact H-Rep polytope representation of $\mathcal{C}$ using *lifted zonotopes*, it may require a combinatorial number of hyperplanes, and may not be

Algorithm 5 Outer-approximation of $\mathcal{C} \ominus \mathcal{S}$

Input: Minuend $\mathcal{C} = (G_C, c_C, A_C, b_C)$ that is full-dimensional and a convex and compact subtrahend $\mathcal{S}$ that is symmetric about any $c_S \in \mathbb{R}^n$

Output: Constrained zonotope $\mathcal{M}^+ \supseteq \mathcal{C} \ominus \mathcal{S}$

1: Compute a convex polyhedron $\mathcal{P} \supseteq \mathcal{C}$ using Algo. 4.
2: Compute a convex polyhedron $\mathcal{M}_{\mathrm{p}}^+ = \mathcal{P} \ominus \mathcal{S}$ via (8).
3: Compute $\mathcal{M}^+ \leftarrow (\mathcal{C} - c_S) \cap \mathcal{M}_{\mathrm{p}}^+$ using (7d) .

practical for large n and/or N_C. Instead, Algo. 4 outer-approximates $\mathcal{C}$ with a convex polyhedron $\mathcal{P}$ that has at most $2N_C$ halfspaces, and can be efficiently computed for $\mathcal{C}$ with large n and N_C without relying on convex optimization solvers. Redundant inequalities in $\mathcal{P}$ may be removed via linear programming [24], if desired.

Remark 3. (H-Rep outer-approximation) *We can modify Algo. 4 in the following ways:*
1) Always return a H-Rep polytope $\mathcal{P} \cap \{x \mid l \leq x \leq u\}$ with l, u computed in (17)*, where $L_P = 2(N_C + n)$.*
2) Reduce approximation error by intersecting $\mathcal{P}$ computed by Algo. 4 with supporting hyperplanes (4) *evaluated along template directions (ray shooting) [10].*
Both modifications incur additional computational cost.

4.2 Outer-approximation of the Pontryagin difference

We now address the outer-approximation part of Prob. 1.

Proposition 4. *For a full-dimensional, constrained zonotopic minuend $\mathcal{C}$ and a convex and compact subtrahend $\mathcal{S} \subset \mathbb{R}^n$ that is symmetric about any $c_S \in \mathbb{R}^n$, Algo. 5 returns a constrained zonotope $\mathcal{M}^+ \supseteq \mathcal{C} \ominus \mathcal{S}$.*

Proof. By Prop. 3 and (8), $\mathcal{M}_{\mathrm{p}}^+$ constructed in Step 2 of Algo. 5 outer-approximates $\mathcal{C} \ominus \mathcal{S}$. Since $\mathcal{S}$ is symmetric about c_S, $(\mathcal{C} - c_S)$ is also an outer-approximation of $\mathcal{C} \ominus \mathcal{S}$ by (6d). We obtain the outer-approximating constrained zonotope $\mathcal{M}^+$ by intersecting these outer-approximations in Step 3 using (7d). □

All steps of Algo. 5 are available in closed-form, when the support function of $\mathcal{S}$ is known in closed-form. Similarly to Algo. 3, Algo. 5 is optimization-free, i.e., it does not require convex optimization solvers, when $\mathcal{S}$ is an ellipsoid, a zonotope, or a convex unions of symmetric intervals (see (5)).

4.3 Sufficient conditions for exactness

We show that the proposed approximations become exact when using an Invertible representation.

Proposition 5. (Sufficient conditions for exactness of polyhedral cover) *For an* Invertible *representation $\mathcal{C}$, Algo. 4 computes a H-Rep polytope $\mathcal{P} = \mathcal{C}$ that is identical to the H-Rep polytope in Prop 1.5.*

Proposition 6. (Sufficient conditions for exactness of Pontryagin difference) *For an* Invertible *representation $\mathcal{C}$, Algo. 3 and 5 provide approximations $\mathcal{M}^-$ and $\mathcal{M}^+$ that satisfy $\mathcal{M}^- = \mathcal{M} = \mathcal{C} \ominus \mathcal{S} = \mathcal{M}^+$.*

See Sec. A.3 and A.4 for the proofs. The exactness results (Prop. 5 and 6) may be attributed to Prop. 1.5. Also, for $\mathcal{C}$ in an Invertible representation, Step 2 of Algo. 5 computes a H-Rep polytope $\mathcal{M}_{\mathrm{p}}^+ = \mathcal{C} \ominus \mathcal{S}$ by Prop. 5. Consequently, instead of Step 3, we can use Algo. 2 to compute $\mathcal{M}^+$ directly from $\mathcal{M}_p^+$.

Algo. 3, 5 address Prob. 1 by Thm. 1 and Prop. 2, 4, 6. Algo. 4 addresses Prob. 2 by Prop. 3, 5.

4.4 Implementation considerations

The use of pseudoinverse $[G_C; A_C]^\dagger$ in Algo. 3, 4, and 5 was motivated by providing closed-form expressions for D_{ii} (20) and v_i (35). However, the computation of $[G_C; A_C]^\dagger$ can be computationally expensive for large N_C and M_C. In practice, it suffices to compute a minimum norm solution of systems of linear equations — a solution Γ in (19) for Step 2 of Algo. 3, a solution ξ to $A_C\xi = b_C$ in Step 4 of Algo. 3, and a solution $V^\top$ to $[G_C; A_C]^\top V^\top = I_{N_C}$ for Step 1 of Algo. 4 (where $V[G_C; A_C]$ is later normalized row-wise in ℓ_1-norm).

We can use QR factorization or complete orthogonal decomposition to compute a minimum norm solution without explicitly computing the psuedoinverse [21, Ch. 12]. Existing algorithms can also exploit sparsity [21, Ch. 12.3]. In Sec. 6 and 7, our `MATLAB` implementation of Algo. 3, 4, and 5 utilizes `lsqminnorm` to compute minimum norm solutions and uses sparse matrices for computational efficiency.

5 Inner-approximation of robust controllable sets

We now address Prob. 3 by inner-approximating the T-step RC set using Algo. 3 and the set recursion (14). We consider both cases described in Prob. 3, characterize the representation complexity of the computed inner-approximations, and show that their representation complexities grow linearly with T.

Throughout this section, we will assume that the input set $\mathcal{U}_t$ and the goal set $\mathcal{G}$ are polytopes, hence, representable as constrained zonotopes, and the additive disturbance set $\mathcal{W}_t$ is a convex and compact set that is symmetric about any $c_W \in \mathbb{R}^p$. Also, we assume that the sets $\mathcal{K}_t$ computed in (14) are full-dimensional for every t.

5.1 Convex polyhedral $\mathcal{X}_t$ and invertible A_t

Given a finite horizon $T \in \mathbb{N}$, we consider the case where A_t in (13) are invertible, and state constraints $\mathcal{X}_t$

Set	Eq. no.	M	$\mathscr{O}$
$\mathcal{K}_{t,\text{inner}}^{\text{interim},1}$	(36a)	$M_{\mathcal{K}_{t+1}}$	$\mathscr{O}_{\mathcal{K}_{t+1}}$
$\mathcal{K}_t^{\text{interim},2}$	(36b)	$M_{\mathcal{K}_{t+1}} + M_{B\mathcal{U}}$	$\mathscr{O}_{\mathcal{K}_{t+1}} + \mathscr{O}_{B\mathcal{U}}$
$\mathcal{K}_t^{\text{interim},3}$	(36c)		
$\mathcal{K}_t$	(36d)	$M_{\mathcal{K}_{t+1}} + M_{B\mathcal{U}} + L_X$	

Table 2
Representation complexity (see Defn. 1) for various sets involved in computing an inner-approximation to the T-step RC set using (36), where $\mathscr{C}(\mathcal{K}_{t+1}) = (M_{\mathcal{K}_{t+1}}, \mathscr{O}_{\mathcal{K}_{t+1}})$ and $\mathscr{C}(B\mathcal{U}) = (M_{B\mathcal{U}}, \mathscr{O}_{B\mathcal{U}})$, and $\mathcal{X}$ is characterized by L_X hyperplanes. Observe that the representation complexity grows by $(M_{BU} + L_X, \mathscr{O}_{B\mathcal{U}})$ with each step of the recursion.

are polyhedra for all $t \in \mathbb{N}_{[0:T-1]}$. Since $\mathcal{X}_t$ can be unbounded, they may not be representable as constrained zonotopes. However, we can still inner-approximate the RC sets as constrained zonotopes using (7d).

For all $t \in \mathbb{N}_{[0:T-1]}$, we break down the set recursion (14) to compute the T-step RC set into four steps:

$$\mathcal{K}_{t,\text{inner}}^{\text{interim},1} \subseteq \mathcal{K}_t^{\text{interim},1} = \mathcal{K}_{t+1} \ominus F_t\mathcal{W}_t, \tag{36a}$$
$$\mathcal{K}_t^{\text{interim},2} = \mathcal{K}_{t,\text{inner}}^{\text{interim},1} \oplus (-B_t\mathcal{U}_t), \tag{36b}$$
$$\mathcal{K}_t^{\text{interim},3} = A_t^{-1}\mathcal{K}_t^{\text{interim},2}, \tag{36c}$$
$$\mathcal{K}_t = \mathcal{K}_t^{\text{interim},3} \cap \mathcal{X}_t. \tag{36d}$$

The recursion (36) is initialized with a constrained zonotope $\mathcal{K}_T = \mathcal{G}$. We use Prop. 2 to compute a constrained zonotope $\mathcal{K}_{t,\text{inner}}^{\text{interim},1}$ in (36a). Then, we compute (36b)–(36d) exactly using (7). Thus, for all $t \in \mathbb{N}_{[0:T-1]}$, the sets $\mathcal{K}_t, \mathcal{K}_{t,\text{inner}}^{\text{interim},1}, \mathcal{K}_t^{\text{interim},2}$, and $\mathcal{K}_t^{\text{interim},3}$ are constrained zonotopes, and $\mathcal{K}^- = \mathcal{K}_0$ is an inner-approximation of the T-step RC set.

Table 2 describes the representation complexity of various constrained zonotopes involved at each step of (36). For ease of discussion, we assume that $\mathcal{X}_t$,$\mathcal{U}_t$, and $\mathcal{W}_t$ are time-invariant, i.e., $\mathcal{X}_t = \mathcal{X}$, $\mathcal{U}_t = \mathcal{U}$, and $\mathcal{W}_t = \mathcal{W}$, for all $t \in \mathbb{N}_{[0:T]}$. Additionally, we assume that $\mathcal{X}$ is characterized by L_X hyperplanes. Given representation complexities $\mathscr{C}(\mathcal{K}_{t+1}) = (M_{\mathcal{K}_{t+1}}, \mathscr{O}_{\mathcal{K}_{t+1}})$ and $\mathscr{C}(B\mathcal{U}) = (M_{B\mathcal{U}}, \mathscr{O}_{B\mathcal{U}})$, the rows of Table 2 follow from Prop. 2, (7b), (7a), and (7d), respectively. With $\mathscr{C}(\mathcal{G}) = (M_{\mathcal{G}}, \mathscr{O}_{\mathcal{G}})$, the representation complexity of the inner-approximation of the T-step RC set is

$$\mathscr{C}(\mathcal{K}^-) = (M_{\mathcal{G}} + T(M_{B\mathcal{U}} + L_X), \mathscr{O}_{\mathcal{G}} + T\mathscr{O}_{B\mathcal{U}}). \tag{37}$$

Observe that the representation complexity of $\mathcal{K}^-$ does not depend on the disturbance set $\mathcal{W}$ due to Prop. 2, and grows linearly with T.

5.2 Polytopic $\mathcal{X}_t$

We now consider the case where the state constraints $\mathcal{X}_t$ are polytopes for all $t \in \mathbb{N}$, and admit a constrained zonotope representation with $\mathscr{C}(\mathcal{X}_t) = (L_{\mathcal{X}_t}, 1)$ when using Algo. 2. Unlike Sec. 5.1, we no longer assume that A_t is invertible.

Similarly to (36), we separate the set recursion (14) into *three* steps performed for all $t \in \mathbb{N}_{[0:T-1]}$:

$$\mathcal{K}_{t,\text{inner}}^{\text{interim},1} \subseteq \mathcal{K}_t^{\text{interim},1} = \mathcal{K}_{t+1} \ominus F_t\mathcal{W}_t, \tag{38a}$$
$$\mathcal{K}_t^{\text{interim},2} = \mathcal{K}_{t,\text{inner}}^{\text{interim},1} \oplus (-B_t\mathcal{U}_t), \tag{38b}$$
$$\mathcal{K}_t = \mathcal{X}_t \cap_{A_t} \mathcal{K}_t^{\text{interim},2}, \tag{38c}$$

where (38c) combines (36c) and (36d) into a single step using (7c). Assuming time-invariance, $\mathscr{C}(\mathcal{X}) = (L_X, 1)$ and the representation complexity of $\mathcal{K}_t$ grows by $(M_{BU} + L_X + n, \mathscr{O}_{B\mathcal{U}})$ at each step of the set recursion (see (7c) and Table 2). Consequently, with $\mathscr{C}(\mathcal{G}) = (M_{\mathcal{G}}, \mathscr{O}_{\mathcal{G}})$, the representation complexity of the inner-approximation of the T-step RC set is

$$\mathscr{C}(\mathcal{K}^-) = (M_{\mathcal{G}} + T(M_{B\mathcal{U}} + L_X + n), \mathscr{O}_{\mathcal{G}} + T\mathscr{O}_{B\mathcal{U}}). \tag{39}$$

Similarly to (37), $\mathscr{C}(\mathcal{K}^-)$ in (39) also grows linearly with T and does not depend on the disturbance set $\mathcal{W}$.

Remark 4. *We can also use the set recursions discussed in Sec. 5.1 and 5.2 in conjunction with Algo. 5 to obtain an outer-approximation to the T-step RC set.*

Remark 5. *In this work, we did not use the exact or approximate reduction techniques [5, 6, 25] that may lower the representation complexity at the expense of additional computation or accuracy or both. On the other hand, it is straightforward to apply these results to the sets computed in this work for a further reduction in the set representation complexity.*

6 Case studies

We now demonstrate the computational efficiency, scalability, and utility of our approach in several case studies. First, we consider two case studies involving low-dimensional systems to illustrate the advantage of the proposed approach in computing time when compared to existing inner-approximating approaches based on constrained zonotopes [9], and exact approaches based on H-Rep and V-Rep polytopes [24]. Then, we discuss the scalability of the approach by computing the RC set for a chain of mass-spring-damper system, and empirically demonstrate that the proposed approach is numerically stable and can compute the RC sets for high-dimensional systems and long horizons.

We perform the presented computations in a standard computer with Intel CPU i9-12900KF processor (3.2 GHz, 16 cores) and 64 GB RAM, running MATLAB 2022b on Windows. We use YALMIP [28], MOSEK [29], and GUROBI [30] to set up and solve the optimization problems. For two-dimensional plots of constrained

zonotopes $\mathcal{C}$, we compute the appropriate H-Rep/V-Rep polytope approximations via support function and vector computations (4) in 100 equi-spaced directions in $\mathbb{R}^2$. We estimate the volume of the sets via grid-based sampling.

6.1 *Double integrator example with polytopic $\mathcal{X}$*

We consider the computation of RC set for a double integrator system with polytopic state constraints $\mathcal{X}$ and an ellipsoidal disturbance set $\mathcal{W}$. The linear time-invariant system matrices are

$$A = \begin{bmatrix} 1 & \Delta T \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} (\Delta T)^2/2 \\ \Delta T \end{bmatrix}, \text{ and } F = I_2,$$

with the sampling period $\Delta T = 0.1$, the input set $\mathcal{U} = [\![-2, 2]\!]$ that is an interval, the disturbance set $\mathcal{W} = (0.1I_2, [0; 0])$ or $\mathcal{W} = (\text{diag}([0.2, 0.04]), [0.1; 0.1])\}$ that is a circle or an ellipsoid respectively, and the state constraints $\mathcal{X} = \mathcal{G} = [\![-2, 2]\!] \times [\![-3, 3]\!]$ that are time-invariant, axis-aligned rectangles.

We generate inner-approximations of the T-step RC set using the recursion in Sec. 5.2 for $T = 20$ with an exact ellipsoidal representation of $\mathcal{W}$ and a zonotopic outer-approximation $\mathcal{W}^+ = (G_W, c_W) \supset \mathcal{W}$ where the Pontryagin difference is inner-approximated using Algo. 3. We also compare the computed sets with the exact sets computed using MPT3 where the vertex-facet enumeration was accomplished using Fourier-Motzkin elimination [24], and the inner-approximations of the RC sets using the two-stage approach with the zonotopic $\mathcal{W}^+$ [9]. We also compute an outer-approximation of the RC sets using Algo. 5, as discussed in Rem. 4.

Table 3 shows that the proposed inner-approximation approach with ellipsoidal $\mathcal{W}$ is about two orders of magnitude faster than the exact approach [24] and the $\mathcal{W}^+$-based approximation via two-stage approach [9], while providing reasonably accurate inner-approximations (about 97% and 77% of the area of the exact RC set in the first and second case respectively). Our approach with zonotopic $\mathcal{W}^+$ is slightly faster than with ellipsoidal $\mathcal{W}$, but it is more conservative due to the zonotopic outer-approximation of the disturbance set. The shorter computation times of the proposed approach are a direct result of Thm. 1 and Prop. 2, since the implementation of the set recursion in Sec. 5.2 can be accomplished in closed-form, i.e., optimization-free. As expected, $(M_{\mathcal{K}_0}, \mathscr{O}_{\mathcal{K}_0})$ of the inner-approximations do not depend on choice of $\mathcal{W}$ (see (39)). The proposed outer-approximation is slower than the inner-approximation, primarily due to the use of linear programming to produce a minimal representation of the convex polyhedron in Step 1 of Algo. 5 to manage the representation complexity. Additionally, $M_{\mathcal{K}_0}$ for outer-approximation is

Method	Area	Compute time		Complexity $\mathscr{C}$		Area	Compute time		Complexity $\mathscr{C}$	
	Ratio	Time (s)	Ratio	$M_{\mathcal{K}_0}$	$\mathscr{O}_{\mathcal{K}_0}$	Ratio	Time (s)	Ratio	$M_{\mathcal{K}_0}$	$\mathscr{O}_{\mathcal{K}_0}$
	$\mathcal{W}$ is a ball (left in Fig. 2)					$\mathcal{W}$ is an ellipsoid (right in Fig. 2)				
Exact [24]	1	2.044	177.39	N/A		1	2.958	176.65	N/A	
Ours $\mathcal{M}^-$	**0.97**	0.012	1	120	11	**0.77**	0.017	1	120	11
Ours $\mathcal{M}^+$	1.67	4.064	352.66	322	11	3.46	4.199	250.78	326	11
	With a zonotope outer-approximation $\mathcal{W}^+ \supset \mathcal{W}$ as the disturbance set									
Ours $\mathcal{M}^-$	0.70	**0.010**	**0.86**	120	11	0.37	**0.014**	**0.84**	120	11
2-stage [9]	0.67	1.594	138.29	120	11	0.22	1.520	90.78	120	11

Table 3
Comparison of various approaches for Sec. 6.1. Our (inner-approximation) approach is about two orders of magnitude faster than existing approaches [9, 24], and generates sufficiently accurate approximations.

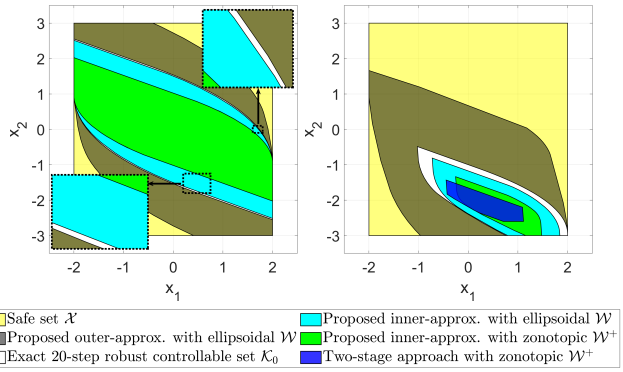

Fig. 2. Robust controllable sets computed using the recursion in Sec. 5.2 for Sec. 6.1 with a ball-shaped $\mathcal{W}$ (left) and an ellipsoidal $\mathcal{W}$ (right). We compare the sets obtained with the proposed approximations to the sets from existing approaches (exact [24] and the two-stage approach [9]). The insets in the left figure show that the proposed approach with ellipsoidal $\mathcal{W}$ (cyan) provides sufficiently accurate inner-approximations of the exact RC set (white).

higher than the inner-approximation due to Step 1 of Algo. 5. For most safe constrained control problems, an inner-approximation of the T-step RC set is sufficient.

Fig. 2 shows that the RC sets and their corresponding inner-approximations, associated with a ball-shaped $\mathcal{W}$ (left) and an ellipsoidal $\mathcal{W}$ (right). As expected, the inner-approximations of the RC set constructed using zonotopic $\mathcal{W}^+$ are more conservative than their ellipsoid-based counterparts in both cases. On the other hand, the proposed inner-approximations with zonotopic $\mathcal{W}^+$ are identical (left) or similar (right) to the inner-approximations produced by the existing two-stage approach [9], while requiring significantly shorter computation time (see Table 3).

6.2 *An example with convex polyhedral $\mathcal{X}$*

We now consider the computation of RC set over a long horizon $T = 100$, similar to [9, Ex. 2]. Consider a stable, discrete-time, linear time-invariant system with matrices

$$A = \begin{bmatrix} 0.99 & 0.02 \\ -0.15 & 0.99 \end{bmatrix}, \quad B = \begin{bmatrix} -0.01 \\ 0.08 \end{bmatrix}, \text{ and } F = I_2,$$

Method	Area	Compute time		Complexity $\mathscr{C}$	
	Ratio	Time (s)	Ratio	$M_{\mathcal{K}_0}$	$\mathscr{O}_{\mathcal{K}_0}$
Exact [24]	1	110.661	1235.87	N/A	
Ours $\mathcal{M}^-$	0.89	**0.090**	**1**	200	202.0
Ours $\mathcal{M}^+$	1.36	158.753	1772.96	1703	953.5
2-stage [9]	**0.92**	10.192	113.82	200	202.0

Table 4
Comparison of various approaches for Sec. 6.2. Our (inner-approximation) approach is about two to three orders of magnitude faster than existing approaches [9, 24], and generates accurate approximations even for a long horizon T.

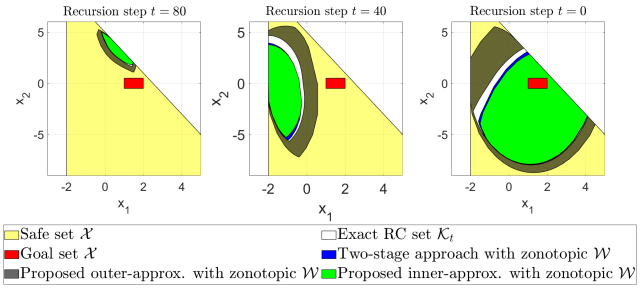

Fig. 3. Snapshots of the 100-step robust controllable sets computed using Sec. 5.1 for Sec. 6.2 at recursion steps $t \in \{0, 40, 80\}$. Our approach computes inner-approximations of the RC set that are similar to those obtained using the exact approach [24] and the two-stage approach [9], with significantly lower computational effort (see Table 4).

and an interval input set $\mathcal{U} = [\![-1.5, 1.5]\!]$, zonotopic disturbance set $\mathcal{W} = (0.01I_2, [0; 0])$, zonotopic goal set $\mathcal{G} = (0.5I_2, [1.5; 0])$, and convex polyhedral, time-invariant state constraints $\mathcal{X} = \{x \mid [-1, 0; 2, 1]x \leq [2; 5]\}$.

Since the state constraints are polyhedral and A is invertible, we generate inner-approximations of the T-step RC set using the recursion in Sec. 5.1. Similarly to Sec. 6.1, we compare the obtained sets with their exact counterparts computed using MPT3 [24] and the inner-approximations obtained using the two-stage approach [9]. We also compute an outer-approximation of the RC sets using Algo. 5.

Table 4 shows that the proposed inner-approximating approach with zonotopic $\mathcal{W}$ is over two to three orders of magnitude faster than the existing approaches [9, 24], while providing reasonably accurate inner-approximations that cover about 89% of the area of the exact RC set, as in Sec. 6.1. The shorter computation time compared to existing approaches is attributed to the optimization-free implementation of Sec. 5.1, by Prop. 2 and Corr. 1. As expected, $(M_{\mathcal{K}_0}, \mathscr{O}_{\mathcal{K}_0})$ for our $\mathcal{M}^-$ and the two-stage approach are identical [9].

Fig. 3 shows the 100-step RC sets computed by various methods at recursion step $t \in \{0, 40, 80\}$. Unlike in Sec. 6.1, the proposed inner-approximation of the RC set in this case is contained in the inner-approximation using the two-stage approach [9]. However, the conservativeness of the proposed approach compared to the two-stage approach [9] appears minimal, covering about 89% vs 92% of the area of the exact RC set.

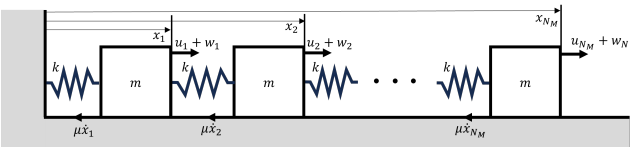

Fig. 4. Chain of N_M mass-spring-damper systems.

6.3 *Scalability: Chain of damped spring-mass systems*

We now demonstrate scalability of the representation complexity for the proposed inner-approximation. Specifically, we compute the RC set of a chain of $N_M \in \mathbb{N}$ homogenous mass-spring-damper systems, see Fig. 4, for a range of chain lengths, i.e., different system dimension, and set recursion lengths, i.e., different horizon T. The chain system has the following continuous-time linear time-invariant dynamics,

$$\ddot{x}_1 = -\frac{2k}{m}x_1 + \frac{k}{m}x_2 - \frac{\mu}{m}\dot{x}_1 + w_1 + u_1, \tag{40a}$$

$$\ddot{x}_{N_M} = -\frac{2k}{m}x_{N_M} + \frac{k}{m}x_{(N_M-1)} - \frac{\mu}{m}\dot{x}_{N_M} + w_{N_M} + u_{N_M}, \tag{40b}$$

$$\ddot{x}_j = -\frac{2k}{m}x_j + \frac{k}{m}(x_{j-1} + x_{j+1}) - \frac{\mu}{m}\dot{x}_j + w_j + u_j, \tag{40c}$$

where $j \in \mathbb{N}_{[2:(N_M-1)]}$. Here, (40) describes a $(2N_M)$-dimensional system parameterized by the spring constant k, the mass m, and the friction coefficient μ. Each spring is actuated by an acceleration input $u_i \in \mathcal{U} \subset \mathbb{R}$ subject to an acceleration disturbance $w \in \mathcal{W} \subset \mathbb{R}$.

After discretizing (40) with sampling time $\Delta T = 0.1$ using zero-order hold, we consider the following computations of T-step RC sets:
1) $n \in \mathbb{N}_{[4:100]}$ with $T = 20$ using Sec. 5.2,
2) $n \in \mathbb{N}_{[4:100]}$ with $T = 40$ using Sec. 5.2,
3) $n \in \mathbb{N}_{[4:50]}$ with $T = 20$ using two-stage approach [9],
4) $n \in \mathbb{N}_{[4:14]}$ with $T = 20$ using exact approach [24].
We use parameters $k = 0.1$, $m = 0.1$, and $\mu = 0.01$, input set $\mathcal{U} = [\![-0.1, 0.1]\!]^{N_M}$, disturbance set $\mathcal{W} = [\![-0.0001, 0.0001]\!]^{N_M}$, and state constraints $\mathcal{X} = \mathcal{G} = ([\![-0.2, 0.2]\!] \times [\![-0.5, 0.5]\!])^{N_M}$.

Fig. 5 shows that the proposed method takes significantly shorter computation time to produce an inner-approximation to the 20-step RC sets, when compared to existing methods [9,24]. Specifically, we observe that our approach takes 12.52 seconds to inner-approximate the 20-step RC set for a 100-dimensional system ($N_M = 50$). On the other hand, the two-stage approach [9] took 649.74 seconds (about 10 minutes) to compute an inner-approximation for the 20-step RC set for much smaller dimensional system $n = 40$ ($N_M = 20$). We encountered

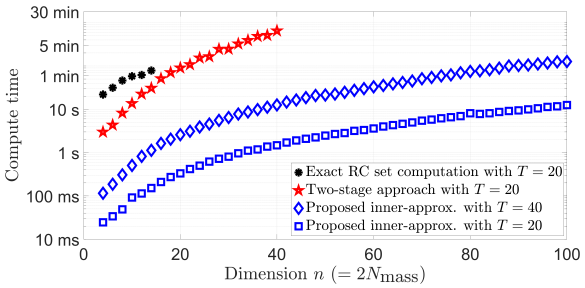

Fig. 5. Time taken by various methods to compute the RC sets for varying system dimension n. The proposed method takes 12.52 seconds to inner-approximate 20-step RC sets for a 100-dimensional system. In contrast, existing methods (the exact computation using MPT3 [24] and the two-stage approach in [9]) require longer computation time to tackle lower dimensional systems. We also report the time taken by the proposed method to inner-approximate 40-step RC sets.

numerical issues for the exact set computation using MPT3 [24] beyond $n = 14$ ($N_M = 7$). As expected, the proposed approach took longer to compute the RC sets for an horizon $T = 40$ compared to the sets for an horizon $T = 20$, but still computed an inner-approximation to the 40-step RC set for the 100 dimensional system in 126.53 seconds (about 2 minutes). The scalability of the proposed approach compared to existing approaches may be attributed to the optimization-free implementation of Sec. 5.2, made possible by Prop. 2 and Corr. 1.

We oberved a moderate growth in the representation complexity of the proposed inner-approximations. For a 10-dimensional system, an inner-approximating constrained zonotope $\mathcal{K}_0$ for the 20-step RC set had a representation complexity of $\mathscr{C}(\mathcal{K}_0) = (620, 11)$ with $n = 10, N_{\mathcal{K}_0} = 730, M_{\mathcal{K}_0} = 620$. As noted in Rem. 5, various reduction techniques may be used to further lower the set representation complexities, if so desired.

7 Application: Abort-safe rendezvous

Abort safety in spacecraft rendezvous [11,13,31] requires that a spacecraft in nominal operation approaching a target must retain the ability to avoid collision with the target in the event of an anomaly or a failure. In [11], we showed that the problem of abort-safe spacecraft rendezvous could be encoded using RC sets, and we computed these sets using H-Rep/V-Rep polytopes. However, such an approach is challenging in high-dimensions and suffers from numerical issues, which motivates the computation of the RC sets using constrained zonotopes. Additionally, to guarantee safety, we require an exact computation or inner-approximation of the RC sets.

In this work, we consider rendezvous to a future Lunar gateway flying in a near-rectilinear halo orbit (NRHO) around the Moon [19]. To minimize the use of fuel, we allow the spacecraft to utilize all 3 degrees of freedom in its approach. We compute six-dimensional RC sets that constrain the rendezvous trajectory in order to guarantee that, in the event of a failure, off-nominal operation of the spacecraft allows for a safe abort maneuver. Additionally, the trajectory must lie in a line-of-sight cone that arises from sensing and communication requirements, and ensures that the Sun stays behind the spacecraft to help in perception of the Lunar gateway.

Nominal dynamics: We obtain the unactuated nonlinear dynamics of the spacecraft in the vicinity of the Lunar gateway by considering Earth and Moon's gravitational forces and dominant perturbations [32]. We linearize the dynamics around the NRHO of the gateway, and discretize the dynamics in T_{sample}-long time intervals to obtain the relative dynamics [31],

$$x_{t+1} = A_t x_t + B_t u_t, \tag{41}$$

with state (position and velocity) $x_t \in \mathbb{R}^6$, input $u_t \in \mathcal{U} \subset \mathbb{R}^3$ models impulsive changes in velocities, and perfect state measurements.

Off-nominal dynamics: We consider three modifications to the nominal dynamics in the event of failure — 1) limited actuation to model the event where the main thrusters fail and the spacecraft is forced to use redundant thrusters like attitude thrusters, 2) process noise to model the resulting actuation uncertainty, and 3) measurement noise to model sensing uncertainty that may increase with the use of redundant thrusters. The need for redundant thrusters is well-known in space applications to ensure safety in off-nominal scenarios [33]. We assume that the process and measurement noises are drawn from pre-determined bounded sets that may be characterized via offline statistical analysis [33].

Specifically, the off-nominal dynamics after a failure event at time t are,

$$z_{k+1|t} = A_t z_{k|t} + B_t(u_{k|t} + w_{k|t}), \tag{42a}$$
$$\hat{z}_{k|t} = z_{k|t} + \eta_{k|t}, \tag{42b}$$

where $z_{k|t}$ is the state after failure at time $k \geq t$ initialized by $z_{t|t} = x_t$ (the nominal state at failure time t), and $w_{k|t} \in \mathcal{W}_{\text{off-nom}} \subset \mathbb{R}^3$ and $\eta_{k|t} \in \mathcal{E}_{\text{off-nom}} \subset \mathbb{R}^6$ are bounded disturbances to the input and post-failure state respectively. The disturbances model the actuation mismatch and sensing limitations that can become prominent after failure. The post-failure input $u_t \in \mathcal{U}_{\text{off-nom}} \subset \mathcal{U}$ where $\mathcal{U}_{\text{off-nom}}$ models the limited actuation available after failure. We consider a feedback controller $\pi : \mathbb{R}^6 \to \mathcal{U}_{\text{off-nom}}$ that provides a post-failure control u in (42) given the current state estimate $\hat{z} \in \mathbb{R}^6$. Let Π be the set of all such controllers.

From (42), the state estimate $\hat{z}_t$ follows the dynamics,

$$\hat{z}_{t+1} = A_t \hat{z}_t + B_t u_t + \phi_t, \tag{43}$$

with disturbance $\phi_t \in \Phi_t = \mathcal{E}_{\text{off-nom}} \oplus (B_t \mathcal{W}_{\text{off-nom}}) \oplus (-A_t \mathcal{E}_{\text{off-nom}})$. From (42b), z_t and $\hat{z}_t$ satisfy

$$z_t \in \hat{z}_t + (-\mathcal{E}_{\text{off-nom}}) \text{ and } \hat{z}_t \in z_t + \mathcal{E}_{\text{off-nom}}. \tag{44}$$

Rendezvous constraints: We consider the problem of navigating the spacecraft to a target set $\mathcal{T} \subset \mathbb{R}^3$ in front of the Lunar gateway, while staying inside a line-of-sight cone $\mathcal{L} \subset \mathbb{R}^3$ originating from the Lunar gateway. The designed nominal rendezvous trajectory must also stay outside a keep-out set $\mathcal{D} \subset \mathbb{R}^3$ around the Lunar gateway during the rendezvous maneuver. Also, for some pre-determined post-failure safety horizon $T_{\text{safe}} \in \mathbb{N}$, the nominal state x_t at any time t must satisfy the abort-safety requirement:

$$\text{(Abort-safety):} \quad \begin{cases} \forall k \in \mathbb{N}_{[t:t+T_{\text{safe}}]},\ \exists \pi_k \in \Pi, \\ \forall w_{k|t} \in \mathcal{W}_{\text{off-nom}},\ \forall \eta_{k|t} \in \mathcal{E}_{\text{off-nom}}, \\ z_{k|t} \text{ in (42) with } u_{k|t} = \pi_k(\hat{z}_{k|t}) \\ \text{satisfies } z_{k|t} \notin \mathcal{D}, \text{ given } z_{t|t} = x_t. \end{cases} \tag{45}$$

Informally, (45) requires the nominal trajectory to permit steering the spacecraft to continue staying outside $\mathcal{D}$ using limited actuation and imperfect state information under perturbed dynamics (42) over a safety horizon of length T_{safe}, in the event of a failure at time t.

Optimal control problem: Given initial state x_0, the optimal control problem is formulated as,

$$\begin{array}{ll} \min & \sum_t \left(\text{dist}(x_t, \mathcal{T})^2 + \lambda \|u_t\|_2\right) \\ \text{s. t.} & \text{Nominal dynamics (41) from } x_0, \\ \forall t, & x_t \in \mathcal{L}, \text{ and } x_t \notin \mathcal{D} \\ \forall t, & x_t \text{ meets abort-safety requirement (45).} \end{array} \tag{46}$$

For $\lambda > 0$, (46) balances the typical goals of rendezvous — approaching the target set $\mathcal{T}$ while limiting the energy spent. We measure the energy spent as $(\Delta v)_t = \|u_t\|_2$.

Enforcement of (Abort-safety) using RC sets: Similarly to [11], we encode the abort-safety requirements using appropriately defined RC sets. Let $\mathcal{S}^{\complement} = \mathbb{R}^3 \setminus \mathcal{S}$ be the complement of a set $\mathcal{S} \subseteq \mathbb{R}^3$.

Proposition 7. (Sufficient condition for Abort-safety) *Consider a H-Rep polytope keep-out set $\mathcal{D} = \cap_{i=1}^{L_D} \mathcal{H}_i$ with L_D halfspaces $\mathcal{H}_i \subset \mathbb{R}^3$, and $\mathcal{E}_{\text{off-nom}}$ that is symmetric about the origin. For any time $s \in \mathbb{N}$, let $\mathcal{K}(s, T_{safe}, \mathcal{H}_i^{\complement} \ominus \mathcal{E}_{\text{off-nom}})$ denote the T_{safe}-step RC set for dynamics (43) characterized by $\{(A_t, B_t, \Phi_t)\}_{t=s}^{s+T_{safe}}$, $\mathcal{U}_{\text{off-nom}}$, and $\mathcal{X}_t = \mathcal{G} = \mathcal{H}_i^{\complement} \ominus \mathcal{E}_{\text{off-nom}}$. Then, x_s satisfies (45) if $x_s \in \cup_{i=1}^{L_D} \left(\mathcal{K}(s, T_{safe}, \mathcal{H}_i^{\complement} \ominus \mathcal{E}_{\text{off-nom}}) \ominus \mathcal{E}_{\text{off-nom}}\right)$.*

See Sec. A.5 for the proof of Prop. 7 using (43) and (44).

We solve (46) using a receding horizon framework. For a finite planning horizon $T_{\text{plan}} \in \mathbb{N}$, the following (non-convex) optimization problem approximates (46),

$$\begin{array}{ll} \underset{\substack{x_{(t+1)|t}, \ldots, x_{(t+T_{\text{plan}})|t} \\ u_{t|t}, \ldots, u_{(T_{\text{plan}}-1)|t}}}{\text{minimize}} & \sum_t \left(\text{dist}(x_t, \mathcal{T})^2 + \lambda \|u_t\|_2\right) \\ \text{subject to} & \text{Dyn. (41) defines } x_{k|t} \text{ given } x_t, \\ \forall k \in \mathbb{N}_{[t+1:t+T_{\text{plan}}]}, & x_{k|t} \in \mathcal{L},\ x_{k|t} \in \bigcup_{i=1}^{L_D} \mathcal{H}_i^{\complement},\ u_{k-1|t} \in \mathcal{U} \\ \forall k \in \mathbb{N}_{[t+1:t+T_{\text{plan}}]}, & x_{k|t} \in \bigcup_{i=1}^{L_D} \mathcal{K}_i'(k, k+T_{\text{safe}}), \end{array} \tag{47}$$

with $\mathcal{K}_i'(k, k+T_{\text{safe}}) \triangleq \mathcal{K}(k, k+T_{\text{safe}}, \mathcal{H}_i^{\complement} \ominus \mathcal{E}_{\text{off-nom}}) \ominus \mathcal{E}_{\text{off-nom}}$. The non-convexity in (47) arises from the *disjunctive constraints* [34].

For a sampling time $T_{\text{sample}} = 20$ minutes, we solve (46) with a planning horizon of 2 hours ($T_{\text{plan}} = 6$) and an abort-safety time horizon of 6 hours ($T_{\text{safe}} = 18$). We consider the nominal control set $\mathcal{U} = [\![-1/3, 1/3]\!]$ (in m/s), off-nominal input set $\mathcal{U}_{\text{off-nom}} = 0.1\mathcal{U}$, post-failure process noise in the ellipsoid $\mathcal{W}_{\text{off-nom}} = (1/60 I_3, 0_{3\times 1})$ (in m/s), and post-failure measurement noise in the ellipsoid $\mathcal{E}_{\text{off-nom}} = (\text{diag}(1, 1, 1, 1/60, 1/60, 1/60), 0_{6\times 1})$ (in m and m/s). We define the origin-centered keep-out set $\mathcal{D} = [\![-100, 100]\!]^3$ (in m) which contains the Lunar gateway [19]. We also define a proper cone characterized by four rays originating from the origin as the line-of-sight cone $\mathcal{L} = \{x \in \mathbb{R}^3 \mid [0, 1, -1; 0, 1, 1; -1, 1, 0; 1, 1, 0]x \leq 0_{4\times 1}\}$. We define an ellipsoidal target set $\mathcal{T} = (0.05 I_3, c_{\text{target}})$ with $c_{\text{target}} = [0.2416; -0.4017; -0.1738]$ and initial state $x_0 = [1.4498; -2.4105; -1.0429; 0.01; 0.01; 0.01]$ such that, from the origin, the target is 0.5 km away and the initial state is 3 km away with non-zero initial velocity. We rotate $\mathcal{D}$ and $\mathcal{L}$ to have the +y-face of $\mathcal{D}$ and the axis of symmetry of $\mathcal{L}$ be aligned with the line segment joining x_0 and c_{target} respectively. The choice of parameters considers a rendezvous approach with the Sun behind the spacecraft, as the gateway flies near the apolune of the NRHO.

The exact computation of $\mathcal{K}_i'(k, k+T_{\text{safe}})$ based on polytopes [24] is challenging, due to the complexity of the calculations involved in the considered problem setting. Therefore, we use the proposed approach for inner-approximating T_{safe}-RC set using constrained zonotopes to enforce abort-safety constraint. Specifically, we use Thm. 1 and Sec. 5.2 to compute constrained zonotopic, inner-approximations of $\mathcal{K}_i'(k, k+T_{\text{safe}})$, and then use big-M formulations to cast the disjunctive constraints in (47) as mixed-integer linear constraints.

Consider L_D constrained zonotopes $\{\mathcal{C}_i\}_{i=1}^{L_D}$ where

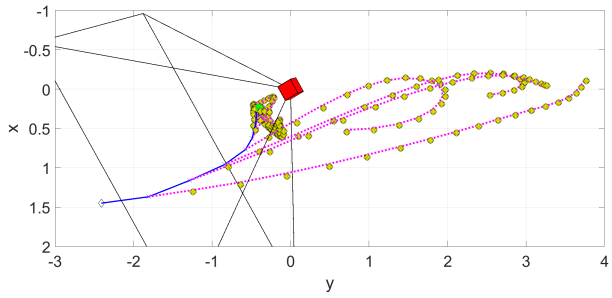

Fig. 6. Designed nominal rendezvous trajectory along with the abort trajectories in case of failures at $t \in \mathbb{N}_{[1:T_{\text{sim}}]}$. The nominal trajectory starts at the initial state (diamond) and reaches the target set $\mathcal{T}$ (green) in $T_{\text{sim}} = 10$ time steps, while staying within the line-of-sight cone $\mathcal{L}$ (black). The abort-safety requirement curves the nominal trajectory away from the keep-out set (red) at all times. The abort trajectories stay outside the keep-out set, despite the presence of disturbances which are adversarially chosen according to (49). See https://youtu.be/6BPmHgxD3OI for more details.

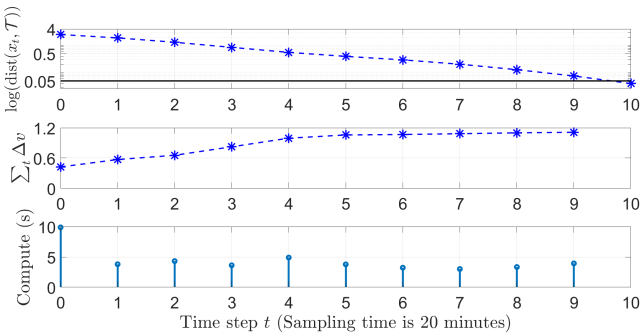

Fig. 7. Evolution of the distance to the target (in log-scale) and cumulative Δv over the course of rendezvous, and computation time for each solution of (47).

$\mathcal{C}_i \subseteq \mathcal{K}'_i(k, k+T_{\text{safe}})$ for each $i \in \mathbb{N}_{[1:L_D]}$ and some $k \in \mathbb{N}_{[t:t+T_{\text{plan}}]}$. Using L_D auxiliary continuous variables $\xi_i \in \mathbb{R}^{N_{C,i}}$ and binary variables $\delta_i \in \{0,1\}$, and a sufficiently large $M > 0$, the following set of $2(n+N_{C,i})+M_{C,i}+1$ mixed-integer linear constraints is sufficient for $x_{k|t} \in \cup_{i=1}^{L_D} \mathcal{K}'_i(k, k+T_{\text{safe}})$ at any $k \in \mathbb{N}_{[t+1:t+T_{\text{plan}}]}$,

$$\begin{aligned} &\forall i \in \mathbb{N}_{[1:L_D]}, \quad \|G_{C,i}\xi_i + c_{C,i} - x_{k|t}\|_\infty \le M(1-\delta_i) \\ &\forall i \in \mathbb{N}_{[1:L_D]}, \quad A_{C,i}\xi_i = b_{C,i},\ \|\xi_i\|_\infty \le 1, \\ &\qquad\qquad \textstyle\sum_{i=1}^{L_D} \delta_i \ge 1. \end{aligned}$$

Similar mixed-integer constraints based on big-M can be used to encode the disjunctive constraint $x_{k|t} \in \cup_{i=1}^{L_D} \mathcal{H}_i^{\complement}$ [34]. Thus, (47) is a mixed-integer quadratic program, which can be solved via off-the-shelf solvers like `GUROBI` [30].

We can also compute an abort-safe control $u_{k|t} = \pi_k(\hat{z}_{k|t})$ for the current state estimate $\hat{z}_{k|t}$ by solving a convex problem,

$$\min_{u_{k|t} \in \mathcal{U}_{\text{off-nom}}} \quad J(u_{k|t}) \text{ s. t. } A_k\hat{z}_{k|t} + B_k u_{k|t} \in \mathcal{K}_{k+1|t} \ominus \Phi_k, \tag{48}$$

where J is a user-specified, convex cost function on the abort-safe control (we choose $J = \|\cdot\|_2$ to minimize post-failure fuel consumption), $\{\mathcal{K}_{k|t}\}_{k=t}^{t+T_{\text{safe}}}$ is the sequence of sets obtained using Sec. 5.2 with $\mathcal{K}_{t+T_{\text{safe}}|t} = \mathcal{H}_i^{\complement} \ominus \mathcal{E}_{\text{off-nom}}$ and $\mathcal{K}(t, T_{\text{safe}}, \mathcal{H}_i^{\complement} \ominus \mathcal{E}_{\text{off-nom}}) = \mathcal{K}_{t|t}$, as prescribed in Prop. 7. We compute the corresponding adversarial disturbance $\phi_{k|t}$ by solving another convex problem,

$$\min_{\phi_{k|t} \in \Phi_k} \quad \text{dist}(A_k\hat{z}_{k|t} + B_k\pi_k(\hat{z}_{k|t}) + \phi_{k|t}, \mathcal{D}). \tag{49}$$

Here, (49) computes $\phi_{k|t}$ that reduces the distance between the next state estimate and the keep-out set. Thus, we approximate the true worst-case disturbance sequence, whose exact computation would have required solving a two-player game, which is computationally difficult in six dimensions [4].

Fig. 6 demonstrates the designed nominal rendezvous trajectory, which takes $T_{\text{sim}} = 10$ time steps (200 minutes) to reach $\mathcal{T}$ with a total Δv of 1.07 m/s. The trajectory design required the computation of 385 18-step RC sets, and the set computation took a total of 7.53 seconds. Fig. 6 also shows the designed abort-safe trajectories originating from each time step of the nominal rendezvous trajectory using the post-failure control (48) and adversarial disturbances (49), along with an outer-approximation of the one-step forward reach set $A_t\hat{z}_{k|t} + B_{k|t}\pi_k(\hat{z}_{k|t}) + \Phi_k$. As expected, the abort-safety requirement (45) is satisfied at all times $t \in \mathbb{N}_{[1:T_{\text{sim}}]}$. As the spacecraft approaches the target, we observe that the conservativeness of our enforcement of the abort-safety requirement (45) via Prop. 7 causes the abort trajectories to cluster in front of the keep out set $\mathcal{D}$. In actual rendezvous missions, the spacecraft would receive a go/no-go decision for docking as it nears the target.

Fig. 7 shows the evolution of the distance to the target set (in log-scale) and the cumulative Δv expended over the course of the rendezvous, as well as the computation time spent solving (47) at each time step $t \in \mathbb{N}_{[0:T_{\text{sim}}]}$. The rendezvous trajectory initially uses moderately high control inputs Δv to steer the spacecraft towards the target while satisfying the abort-safety requirements, and then utilizes the momentum to reach the target set with minimal additional control inputs, as expected. The rendezvous trajectory maintains abort-safety using the constrained zonotope-based constraints computed with the method proposed in this paper.

8 Conclusion

We presented novel theory and algorithms to approximate the Pontryagin difference between a constrained zonotopic minuend and a symmetric, convex, and compact subtrahend. For broad classes of subtrahends, our approach admits closed-form expressions for the inner-approximation. We use these algorithms for a tractable and scalable computation of an inner-(and outer-)approximation of the robust controllable set for discrete-time linear systems with additive disturbance sets that are symmetric, convex, and compact and subject to linear state and input constraints. We showed by numerical simulations that the proposed approach provides non-trivial inner-approximations of the RC sets with significantly shorter computation times than the previously published methods.

A Proofs

A.1 Proof of Prop. 1

Proof of 1) Assume for contradiction that, G_C does not have full row rank for some full-dimensional constrained zonotope $\mathcal{C} = (G_C, c_C, A_C, b_C)$. Then, there exists a vector $\alpha_{G_C} \in \mathbb{R}^n,\ \alpha_{G_C} \neq 0$ such that $\alpha_{G_C}^\top G_C = 0$. From (2), for every $x \in \mathcal{C}$, there exists $\xi \in \mathcal{B}_\infty(A_C, b_C)$ such that $G_C\xi = x - c_C$. Consequently, $\mathcal{C} \subset \{x \mid \alpha_{G_C}^\top x = \alpha_{G_C}^\top c_C\}$ since $\alpha_{G_C}^\top(x - c_C) = \alpha_{G_C}^\top G_C\xi = 0$ for every $x \in \mathcal{C}$. In other words, the affine dimension of $\mathcal{C}$ is smaller than n. However, this is a contradiction since $\mathcal{C}$ is full-dimensional. Thus, G_C has full row rank for every full-dimensional $\mathcal{C} = (G_C, c_C, A_C, b_C)$.

Proof of 3) We now show that Algo. 1 converts any full-dimensional $\mathcal{C} = (G_C, c_C, A_C, b_C)$ into a MinRow representation. From 1), $G'_C = G_C$ has full row rank. Consider A'_C, b'_C in Step 2 of Algo. 1 with $[A'_C, b'_C] \in \mathbb{R}^{M'_C \times (N_C+1)}$. Then, $M'_C = \text{rank}([A'_C, b'_C]) = \text{rank}([A_C, b_C]) \leq M_C$. It suffices to show that $\mathcal{C} = (G_C, c_C, A'_C, b'_C)$ and $[G_C; A'_C]$ has full row rank.

Without loss of generality, assume that A'_C, b'_C are the first M'_C rows of $[A_C, b_C]$. Since $\text{rank}([A_C, b_C]) = \text{rank}([A'_C, b'_C])$, every row of $[A_C, b_C]$ is a linear combination of the rows of $[A'_C, b'_C]$. In other words, there exists $E \in \mathbb{R}^{(M_C - M_C{}') \times M_C{}'}$ such that $[A_C, b_C] = [I_{M_C{}'}; E][A'_C, b'_C]$. The matrix $[I_{M_C{}'}; E]$ has full column rank implying that $[I_{M_C{}'}; E]y = 0$ if and only if $y = 0$ [21, Ch. 11]. Thus, $\{\xi \mid A_C\xi = b_C\} = \{\xi \mid A'_C\xi = b'_C\}$, since for any ξ such that $A_C\xi = b_C$, $[A_C, b_C][\xi; -1] = 0 \Leftrightarrow [I_{M_C{}'}; E][A'_C, b'_C][\xi; -1] = 0 \Leftrightarrow [A'_C, b'_C][\xi; -1] = 0$. Therefore, $\mathcal{B}_\infty(A_C, b_C) = \mathcal{B}_\infty(A'_C, b'_C)$ and $\mathcal{C} = (G_C, c_C, A_C, b_C) = (G_C, c_C, A'_C, b'_C)$.

Since full-dimensional constrained zonotopes are non-empty, $\{\xi \mid A'_C\xi = b'_C\}$ is non-empty and $\text{rank}(A'_C) = \text{rank}([A'_C, b'_C]) = M'_C$. Assume, for contradiction, that the matrix $[G_C; A'_C]$ has linearly dependent rows. In other words, there exists $\beta_1 \in \mathbb{R}^n,\ \beta_1 \neq 0$ and $\beta_2 \in \mathbb{R}^{M_C{}'},\ \beta_2 \neq 0$ s.t.,

$$[\beta_1^\top, \beta_2^\top][G_C; A'_C] = 0 \equiv \beta_1^\top G_C + \beta_2^\top A'_C = 0. \quad \text{(A.1)}$$

We know $\beta_1^\top G_C \neq 0$ and $\beta_2^\top A'_C \neq 0$, since rows of G_C and A'_C are linearly independent among themselves. From (1b), for all $x \in \mathcal{C}$, there exists $\xi \in \mathbb{R}^{N_C}$ s.t.,

$$[G_C; A'_C]\xi = [x - c_C; b'_C] \text{ and } \|\xi\|_\infty \leq 1. \quad \text{(A.2)}$$

By (A.1) and (A.2), $\mathcal{C} \subset \{x \mid \beta_1^\top(x - c_C) + \beta_2^\top b'_C = 0\}$, which is a contradiction since $\mathcal{C}$ is full-dimensional. Thus, all rows of $[G_C; A'_C]$ are linearly independent, and (G_C, c_C, A'_C, b'_C) is a MinRow representation of $\mathcal{C}$.

Proof of 2) Since constrained zonotopes are a representation of polytopes [5, Thm. 1], the proof of 3) also shows that every full-dimensional polytope admits a MinRow representation. We now show that the reverse is also true, i.e., any non-empty polytope $\mathcal{C}$ in MinRow representation (G_C, c_C, A_C, b_C) is full-dimensional. Assume, for contradiction, that $\mathcal{C}$ is not full-dimensional. Then, there exists an affine set characterized by $\alpha \in \mathbb{R}^n, \alpha \neq 0$ and $\beta \in \mathbb{R}$ such that $\mathcal{C} \subset \{x \mid \alpha^\top x = \beta\}$. Since $\mathcal{C}$ is non-empty, $\mathcal{C} = \mathcal{C} \cap \{x \mid \alpha^\top x = \beta\}$. From [6], $\mathcal{C} = (G_C, c_C, [A_C; \alpha^\top G_C], [b_C; \beta - \alpha^\top c_C]) = (G_C, c_C, A_C, b_C)$. Consequently, there exists some $\gamma \in \mathbb{R}^{M_C}, \gamma \neq 0$ such that $\alpha^\top G_C = \gamma^\top A_C$ and $\beta - \alpha^\top c_C = \gamma^\top b_C$, a contradiction since $[G_C; A_C]$ has full row rank. Thus, $\mathcal{C}$ is full-dimensional, which completes the proof.

Proof of 4) Algo. 2 follows the steps of [5, Thm. 1] with the zonotope $\mathcal{Z}$ in Step 1 defined as a rectangular outer-approximation with $\mathcal{C} \subseteq \{x \in \mathbb{R}^n \mid l \leq x \leq u\}$, and $\sigma \in \mathbb{R}^{L_C}$ defined in Step 2 using (4) such that $\mathcal{P} = \{x \in \mathcal{Z} \mid \sigma \leq Hx \leq k\} \subset \mathbb{R}^n$. Thus, (G_C, c_C, A_C, b_C) defined in Step 3 is a constrained zonotope representation of the given H-Rep polytope $\mathcal{C}$. Since $\mathcal{C}$ is full-dimensional, $l < u$ and $\sigma < k$. Consequently,

$$\begin{bmatrix} G_C \\ A_C \end{bmatrix} = \begin{bmatrix} \text{diag}\left(\frac{u-l}{2}\right) & 0_{n\times M} \\ H\,\text{diag}\left(\frac{u-l}{2}\right) & \text{diag}\left(\frac{\sigma-k}{2}\right) \end{bmatrix}, \quad \text{(A.3)}$$

is a lower triangular matrix with non-zero diagonal entries (and thereby, invertible). This completes the proof.

Proof of 5) Any Invertible representation satisfies

$$\begin{aligned} \mathcal{C} &= \left\{x \middle| \exists \xi \in \mathbb{R}^{N_C},\ \|\xi\|_\infty \leq 1,\ [G_C; A_C]\,\xi = [x - c_C; b_C]\right\} \\ &= \left\{x \middle| \left\| [G_C; A_C]^{-1}\,[x - c_C; b_C] \right\|_\infty \leq 1\right\}. \end{aligned} \quad \text{(A.4)}$$

We obtain (18) by rearranging terms in (A.4). □

A.2 Proof of Prop. 3

Since $\mathcal{C}$ is full-dimensional, it is non-empty. From (1b) and strong duality (via refined Slater's condition [22]),

$$\mathcal{C} = \left\{ x \;\middle|\; \sup_{\substack{\nu \in \mathbb{R}^{n+M_C} \\ \|[G_C; A_C]^\top \nu\|_1 \le 1}} \nu^\top [x - c_C; b_C] \le 1 \right\}. \tag{A.5}$$

For every $i \in \mathbb{N}_{[1:N_C]}$, define ν_i^* as the minimum-norm solution to $[G_C; A_C]^\top \nu = e_i$. By Prop. 1.2, ν_i^* is available in closed-form, where

$$\nu_i^* = \left([G_C; A_C][G_C; A_C]^\top\right)^{-1} [G_C; A_C] e_i = \left([G_C; A_C]^\dagger\right)^\top e_i,$$

for every $i \in \mathbb{N}_{[1:N_C]}$. Step 1 of Algo. 4 (see (35)) rescales ν_i^* to ensure that $[G_C; A_C]^\top \nu_i^*$ has a unit ℓ_1-norm to obtain $v_i^\top$. Thus, $\pm v_i^\top$ are feasible for (A.5) for every $i \in \mathbb{N}_{[1:N_C]}$, and using (A.5),

$$\mathcal{C} \subseteq \mathcal{P} \triangleq \left\{ x \mid \left\| V^\top [x - c_C; b_C] \right\|_\infty \le 1 \right\}, \tag{A.6}$$

with $V = [\nu_1^*; \ldots; \nu_{N_C}^*]$. Steps 2, 3 of Algo. 4 define $\mathcal{P} = \{x \mid Hx \le k\}$ with $H \in \mathbb{R}^{2N_C \times n}$ and $k \in \mathbb{R}^{2N_C}$. □

A.3 Proof of Prop. 5

From (A.4), an INVERTIBLE representation $\mathcal{C}$ may also be expressed as the following H-Rep polytope,

$$\mathcal{C} = \left\{ x \;\middle|\; \begin{array}{c} \forall i \in \mathbb{N}_{[1:N_C]},\ \forall \delta \in \{-1, 1\}, \\ \delta e_i^\top [G_C; A_C]^{-1} [x - c_C; b_C] \le 1 \end{array} \right\}. \tag{A.7}$$

Here, v_i defined in Step 1 of Algo. 4 also simplifies to $e_i^\top [G_C; A_C]^{-1}$ when $[G_C; A_C]$ is invertible [21, Sec. 11.5]. Thus, Algo. 4 returns a H-Rep polytope $\mathcal{P}$ that coincides with (A.7) (thereby, equal to $\mathcal{C}$). The proof is completed with the observation that (A.7) is identical to (A.4). □

A.4 Proof of Prop. 6

Exactness of $\mathcal{M}^+$) As seen from Prop. 5, Algo. 4 computes an exact H-Rep polytope, given an INVERTIBLE representation $\mathcal{C}$. Since the rest of steps of Algo. 5 are exact, $\mathcal{M}^+ = \mathcal{C} \ominus \mathcal{S}$.

Exactness of $\mathcal{M}^-$) For an INVERTIBLE representation $\mathcal{C}$, Γ prescribed by Prop. 2 is

$$\Gamma = [G_C; A_C]^{-1} [I_n; 0_{M_C \times n}], \tag{A.8}$$

by [21, Sec. 11.5]. We show that $\mathcal{M} = \mathcal{C} \ominus \mathcal{S}$ is an affine transformation of $\mathcal{C}_L$ defined in the proof of Thm. 1 (see (21)).

$$\mathcal{M} = \left\{ x \;\middle|\; \begin{array}{c} \forall s \in \mathcal{S}_0,\ \forall i \in \mathbb{N}_{[1:N_C]},\ \forall \delta \in \{-1, 1\}, \\ \delta e_i^\top [G_C; A_C]^{-1} [x + s + c_S - c_C; b_C] \le 1 \end{array} \right\} \tag{A.9}$$

$$= \left\{ x \;\middle|\; \begin{array}{c} \forall s \in \mathcal{S}_0,\ \forall i \in \mathbb{N}_{[1:N_C]},\ \forall \delta \in \{-1, 1\}, \\ \delta e_i^\top \left(\Gamma x + \Gamma s + [G_C; A_C]^{-1} [-c_{M^-}; b_C]\right) \le 1 \end{array} \right\} \tag{A.10}$$

$$= \left\{ x \;\middle|\; \begin{array}{c} \forall i \in \mathbb{N}_{[1:N_C]},\ \forall \delta \in \{-1, 1\}, \\ \delta e_i^\top \left(\Gamma x + [G_C; A_C]^{-1} [-c_{M^-}; b_C]\right) \le 1 - \rho_{\mathcal{S}_0}(\Gamma^\top e_i) \end{array} \right\} \tag{A.11}$$

$$= \left\{ x \;\middle|\; \begin{array}{c} \xi \triangleq \Gamma x + [G_C; A_C]^{-1} [-c_{M^-}; b_C], \\ \forall i \in \mathbb{N}_{[1:N_C]},\ \forall \delta \in \{-1, 1\},\ \delta e_i^\top \xi \le D_{ii} \end{array} \right\} \tag{A.12}$$

$$= \left\{ x \;\middle|\; \begin{array}{c} G_C \xi + c_{M^-} = x,\ A_C \xi = b_C, \\ \forall i \in \mathbb{N}_{[1:N_C]},\ \forall \delta \in \{-1, 1\},\ \delta e_i^\top \xi \le D_{ii} \end{array} \right\} \tag{A.13}$$

$$= \left\{ G_C \xi + c_{M^-} \;\middle|\; A_C \xi = b_C,\ \forall i \in \mathbb{N}_{[1:N_C]},\ |e_i^\top \xi| \le D_{ii} \right\}$$

$$= G_C \mathcal{C}_L + c_{M^-} = \mathcal{M}^-. \tag{A.14}$$

Here, (A.9) follows from (6d) and (A.7) in Sec. A.3, (A.10) follows from (A.8), (A.11) follows from encoding the condition for all $s \in \mathcal{S}_0$ using the support function of $\mathcal{S}_0$, (A.12) follows from the definition of D_{ii} in (20), (A.13) follows from expressing ξ as a solution of linear equations $[G_C; A_C]\xi = [x - c_{M^-}; b_C]$ with invertible $[G_C; A_C]$, and (A.14) follows from the definition of $\mathcal{C}_L$ in (29) (see the proof of Thm. 1). Consequently, for an INVERTIBLE representation $\mathcal{C}$, Prop. 2 provides an exact characterization of $\mathcal{C} \ominus \mathcal{S}$. □

A.5 Proof of Prop. 7

From [27, Thm. 2.1(iii)], $(\mathcal{U} \ominus \mathcal{V}) \oplus \mathcal{V} \subseteq \mathcal{U}$ for any sets $\mathcal{U}, \mathcal{V}$. Let a failure occur at some time $s \in \mathbb{N}$. Using (44) and [27, Thm. 2.1(iii)], for some $i \in \mathbb{N}_{[1:L_D]}$, $\hat{z}_{s|s} = x_s \in \mathcal{K}(s, T_{\text{safe}}, \mathcal{H}_i^{\complement} \ominus \mathcal{E}_{\text{off-nom}}) \ominus \mathcal{E}_{\text{off-nom}}$, which implies that $\hat{z}_{s|s} \in \mathcal{K}(s, T_{\text{safe}}, \mathcal{H}_i^{\complement} \ominus \mathcal{E}_{\text{off-nom}})$. From Defn. 2, for every time step $k \in \mathbb{N}_{[s:s+T_{\text{safe}}]}$, there exists $\pi_k \in \Pi$ such that $u_{k|s} = \pi_k(\hat{z}_{k|s}) \in \mathcal{U}_{\text{off-nom}}$ steers the state estimate according to the dynamics (43) to satisfy $\hat{z}_{k|s} \in \mathcal{H}_i^{\complement} \ominus \mathcal{E}_{\text{off-nom}}$, despite the disturbance $\phi_{k|s} \in \Phi_k$. By (44) and [27, Thm. 2.1(iii)], $\hat{z}_{k|s} \in \mathcal{H}_i^{\complement} \ominus \mathcal{E}_{\text{off-nom}}$ implies that $z_{k|s} \in \mathcal{H}_i^{\complement}$ (and thereby, $z_{k|s} \notin \mathcal{D}$) for all $k \in \mathbb{N}_{[s:s+T_{\text{safe}}]}$, which completes the proof. □

References

[1] W. Langson, I. Chryssochoos, S. Raković, and D. Q. Mayne, "Robust model predictive control using tubes," *Automatica*, vol. 40, no. 1, pp. 125–133, 2004.

[2] D. Mayne, M. Seron, and S. Raković, "Robust model predictive control of constrained linear systems with bounded disturbances," *Automatica*, vol. 41, no. 2, pp. 219–224, 2005.

[3] F. Borrelli, A. Bemporad, and M. Morari, *Predictive control for linear and hybrid systems*. Cambridge Univ. Press, 2017.

[4] D. Bertsekas and I. Rhodes, "On the minimax reachability of target sets and target tubes," *Automatica*, vol. 7, pp. 233–247, 1971.

[5] J. Scott, D. Raimondo, G. Marseglia, and R. Braatz, "Constrained zonotopes: A new tool for set-based estimation and fault detection," *Automatica*, vol. 69, pp. 126–136, 2016.

[6] V. Raghuraman and J. Koeln, "Set operations and order reductions for constrained zonotopes," *Automatica*, 2022.

[7] F. Xu, S. Olaru, and M. Seron, "Observer gain optimization for minimization of minimal robust positively invariant set and invariant set-based fault detection," *Automatica*, 2024.

[8] F. Gruber and M. Althoff, "Scalable robust safety filter with unknown disturbance set," *IEEE Trans. Auto. Ctrl.*, vol. 68, no. 12, pp. 7756–7770, 2023.

[9] L. Yang, H. Zhang, J. Jeannin, and N. Ozay, "Efficient backward reachability using the Minkowski difference of constrained zonotopes," *IEEE Trans. Comp.-Aided Design Integ. Circ. Syst.*, vol. 41, no. 11, pp. 3969–3980, 2022.

[10] J. Gleason, A. Vinod, and M. Oishi, "Lagrangian approximations for stochastic reachability of a target tube," *Automatica*, vol. 125, 2021.

[11] A. Vinod, A. Weiss, and S. Di Cairano, "Abort-safe spacecraft rendezvous under stochastic actuation and navigation uncertainty," in *Proc. Conf. Dec. & Ctrl.*, 2021.

[12] A. Vinod, J. Gleason, and M. Oishi, "SReachTools: a MATLAB stochastic reachability toolbox," in *Proc. Hybrid Syst.: Comp. & Ctrl.*, pp. 33–38, 2019.

[13] D. Marsillach, S. Di Cairano, and A. Weiss, "Abort-safe spacecraft rendezvous on elliptic orbits," *IEEE. Trans. Ctrl. Syst. Tech.*, vol. 31, pp. 1133 – 1148, 2022.

[14] H. Ahn, K. Berntorp, P. Inani, A. Ram, and S. Di Cairano, "Reachability-based decision-making for autonomous driving: Theory and experiments," *IEEE. Trans. Ctrl. Syst. Tech.*, vol. 29, no. 5, pp. 1907–1921, 2020.

[15] N. Malone, H. Chiang, K. Lesser, M. Oishi, and L. Tapia, "Hybrid dynamic moving obstacle avoidance using a stochastic reachable set-based potential field," *IEEE Trans. Rob.*, vol. 33, no. 5, pp. 1124–1138, 2017.

[16] F. Blanchini and S. Miani, *Set-theoretic analysis of dynamic systems*. Springer International Publishing, 2015.

[17] M. Althoff, G. Frehse, and A. Girard, "Set propagation techniques for reachability analysis," *Annual Rev. Ctrl., Rob., & Auto. Syst.*, vol. 4, no. 1, pp. 369–395, 2021.

[18] E. C. Kerrigan, *Robust constraint satisfaction: Invariant sets and predictive control*. University of London, 2000.

[19] NASA, "Lunar gateway," 2023. `https://www.nasa.gov/mission/gateway/` (Last accessed: 2023).

[20] M. Althoff, "An introduction to CORA," in *Proc. Sec. Verif. Cont. Hybrid Syst.*, pp. 120–151, December 2015.

[21] S. Boyd and L. Vandenberghe, *Introduction to Applied Linear Algebra: Vectors, Matrices, and Least Squares*. Cambridge Univ. Press, 2018.

[22] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge Univ. Press, 2004.

[23] S. Sadraddini and R. Tedrake, "Linear encodings for polytope containment problems," in *Proc. Conf. Dec. & Ctrl.*, pp. 4367–4372, IEEE, 2019.

[24] M. Herceg, M. Kvasnica, C. Jones, and M. Morari, "Multi-Parametric Toolbox 3.0," in *Proc. Euro. Ctrl. Conf.*, 2013.

[25] A. Kopetzki, B. Schürmann, and M. Althoff, "Methods for order reduction of zonotopes," in *Proc. Conf. Dec. & Ctrl.*, pp. 5626–5633, IEEE, 2017.

[26] A. Girard and C. Guernic, "Efficient reachability analysis for linear systems using support functions," *IFAC Proc. Vol.*, vol. 41, no. 2, pp. 8966–8971, 2008.

[27] I. Kolmanovsky and E. Gilbert, "Theory and computation of disturbance invariant sets for discrete-time linear systems," *Math. Prob. in Engg.*, vol. 4, pp. 317–367, 1998.

[28] J. Lofberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in *IEEE Intn'l Conf. Rob. Autom.*, pp. 284–289, 2004.

[29] MOSEK, *The MOSEK optimization toolbox for MATLAB manual. Version 10.0.*, 2022.

[30] Gurobi Opt., LLC, "Gurobi Optimizer Reference Manual." `https://www.gurobi.com` (Last accessed: 2023).

[31] D. Marsillach, S. Di Cairano, U. Kalabić, and A. Weiss, "Fail-safe spacecraft rendezvous on near-rectilinear halo orbits," in *Proc. Amer. Ctrl. Conf.*, pp. 2980–2985, IEEE, 2021.

[32] V. Muralidharan, A. Weiss, and U. Kalabic, "Control strategy for long-term station-keeping on near-rectilinear halo orbits," in *AIAA Scitech*, p. 1459, 2020.

[33] W. Fehse, *Automated rendezvous and docking of spacecraft*, vol. 16. Cambridge Univ. Press, 2003.

[34] A. Bemporad and M. Morari, "Control of systems integrating logic, dynamics, and constraints," *Automatica*, vol. 35, 1999.

Abraham P. Vinod received the B.Tech. and M.Tech. degrees in electrical engineering from the Indian Institute of Technology, Madras (IITM), Chennai, India, in 2014 and the Ph.D. degree in electrical engineering from the University of New Mexico, Albuquerque, NM, USA, in 2018. He is currently a Principal Research Scientist at Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA, USA. His main research interests are in the areas of constrained control under uncertainty, multi-agent systems, and learning.

Avishai Weiss received the B.S. degree in electrical engineering and the M.S. degree in aeronautics and astronautics from Stanford University, Stanford, CA, USA, in 2008 and 2009, respectively, and the Ph.D. degree in aerospace engineering from the University of Michigan, Ann Arbor, MI, USA, in 2013. He is currently a Senior Principal Research Scientist at Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA, USA. His main research interests are in the areas of spacecraft control, constrained control, and motion planning.

Stefano Di Cairano received the Master's (Laurea) and Ph.D. degrees in information engineering from the University of Siena, Siena, Italy, in 2004 and 2008, respectively. He is currently a Distinguished Research Scientist at Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA, USA. His main research interests are in the optimization-based control and decision-making strategies for complex mechatronic systems. He was an Associate Editor of the IEEE Transactions on Control Systems Technology.