Efficient Backward Reachability using the Minkowski Difference of Constrained Zonotopes

Liren Yang, *Member, IEEE,* Hang Zhang, Jean-Baptiste Jeannin, Necmiye Ozay, *Senior Member, IEEE*

***Abstract*—Backward reachability analysis is essential to synthesizing controllers that ensure the correctness of closed-loop systems. This paper is concerned with developing scalable algorithms that under-approximate the backward reachable sets, for discrete-time uncertain linear and nonlinear systems. Our algorithm sequentially linearizes the dynamics, and uses constrained zonotopes for set representation and computation. The main technical ingredient of our algorithm is an efficient way to under-approximate the Minkowski difference between a constrained zonotopic minuend and a zonotopic subtrahend, which consists of all possible values of the uncertainties and the linearization error. This Minkowski difference needs to be represented as a constrained zonotope to enable subsequent computation, but, as we show, it is impossible to find a polynomial-size representation for it in polynomial time. Our algorithm finds a polynomial-size under-approximation in polynomial time. We further analyze the conservatism of this under-approximation technique, and show that it is exact under some conditions. Based on the developed Minkowski difference technique, we detail two backward reachable set computation algorithms to control the linearization error and incorporate nonconvex state constraints. Several examples illustrate the effectiveness of our algorithms.**

***Index Terms*—Computational geometry, backward reachability analysis, Minkowski difference, constrained zonotope.**

I. Introduction

BACKWARD reachability analysis is concerned with finding a set of states (called the backward reachable set, BRS for short), from where a proper control strategy can steer the system's trajectories into a prescribed target region in finite time. The computation of BRSs is central to many control synthesis problems with reachability [1], [2], safety [3], [4] or even more complex temporal logic requirements [5], and can be used to seek critical test cases for closed-loop systems with complex controllers in the loop [6], [7]. Whenever the exact computation is hard, an under-approximation can still be used to define a conservative strategy that accomplishes the reachability task. For systems that exhibit modeling error or are affected by environmental uncertainties, the target region should be reached in a guaranteed manner, regardless of these uncertainties. This leads to a conservative analysis and hence smaller BRSs. For linear systems with additive disturbances, this amounts to a Minkowski difference step in the sequential computation of BRSs [1]. For nonlinear systems, this is achieved by shrinking the target set [8], [9], which can be implemented by Minkowski subtracting a set that over-approximates the impact of the linearization error and disturbances. This shrinking step is absent in the forward reachability analysis, for which there is a sizable literature focusing on over-approximation (see [10] and the references therein). However, to under-approximate the BRSs under uncertainties by employing those forward computation techniques (e.g., [11], [12]), the shrinking step is necessary.

Minkowski Difference: Since the late 60s, a simple approach using support functions is known to compute the exact Minkowski difference (in halfspace representation, H-Rep for short) between a polyhedral minuend (in H-Rep) and a compact subtrahend [13]. For a thorough discussion on this subject, see [14]. For high-dimensional polyhedra, unfortunately, H-Reps are not suitable for other operations such as affine transformation and Minkowski addition. This is because an H-Rep's complexity may grow exponentially after these operations [15]. For example, the off-the-shelf tool MPT3 [16] may return an error when computing the Minkowski addition between two 4-D polytopes. For applications like reachability analysis that extensively involves such operations, algorithms can be made more scalable at the cost of generality, by considering a special class of polyhedra called zonotopes. A zonotope can be expressed by its generator representation (G-Rep for short), which is more suitable for affine transformation and Minkowski addition. The Minkowski difference, however, is not as easy to compute when the minuend is in G-Rep. Compared to other operations, the problem of Minkowski-subtracting a set from a zonotopic minuend (in G-Rep) receives less attention, and is first studied in [17], where the subtrahend is also assumed to be a zonotope (in G-Rep). The exact Minkowski difference is not necessarily a zonotope, but a zonotopic under-approximation can still be found efficiently [18], [19] using the encoding techniques developed in [20]. Based on these developments, a scalable backward reachability algorithm is obtained for linear systems with additive disturbances in [19].

Manuscript received April 07, 2022; revised June 11, 2022; accepted July 05, 2022. This article was presented at the International Conference on Embedded Software (EMSOFT) 2022 and appeared as part of the ESWEEK-TCAD special issue. This work is supported by the NSF grants ECCS-1553873 and CCF-1918123, and the ONR grant N000141812501.

L. Yang is with the School of Artificial Intelligence and Automation, Huazhong University of Science and Technology, Wuhan 430074, China lirenyang@hust.edu.cn. H. Zhang is with the Department of Mechanical Engineering, University of Wisconsin-Madison, Madison, WI 53706, USA hang.zhang@wisc.edu. J.-B. Jeannin is with the Department of Aerospace Engineering, University of Michigan, Ann Arbor, MI 48105, USA jeannin@umich.edu. N. Ozay is with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48105, USA necmiye@umich.edu.

Constrained Zonotopes: To enjoy the same computational advantages as zonotopes (and their G-Reps) while achieving the generality of polyhedra, a new set representation called constrained generator representation (CG-Rep for short) is proposed in [21]. A set expressible by CG-Rep is called a constrained zonotope. Not only can affine transformation and Minkowski addition of constrained zonotopes be done easily via CG-Rep manipulation, so can intersection, under which zonotopes are not even closed. Moreover, all polytopes (i.e., bounded polyhedra) are expressible by CG-Rep. Therefore, constrained zonotopes (in CG-Reps) serve as an efficient tool for set-based control and estimation. They are more general than zonotopes and are particularly suitable to deal with state constraints. However, the Minkowski difference operation, which is necessary for BRS computation, is difficult for constrained zonotopes. In fact, we show that no polynomial-time algorithm can find a polynomial-size CG-Rep of the Minkowski difference between a constrained zonotopic minuend (in CG-Rep) and a zonotopic subtrahend (in G-Rep), unless P = NP. Neither is there, to the best of our knowledge, an efficient way to compute a polynomial-size under-approximation. This prohibits the use of constrained zonotopes for BRS computation under uncertainties because a compact representation of the BRS is essential for its efficient end uses (e.g., checking if a state belongs to the BRS and deriving the control law accordingly).

Contributions: In this paper, we use constrained zonotopes to develop scalable algorithms that under-approximate the BRSs for discrete-time nonlinear systems. Our approach is based on sequential linearization, and the linearization error is incorporated with a Minkowski difference step. Our technical contributions are summarized as follows.

i) We propose an efficient way to under-approximate the Minkowski difference between a constrained zonotopic minuend (in CG-Rep) and a zonotopic subtrahend (in G-Rep). Our approach is optimization-based. We show that a naïve use of the encoding from [20] leads to a bilinear program, but by extending the two-step approach proposed in [19], an under-approximation can be found via a linear program. The size of this linear program is polynomial in that of the minuend's and the subtrahend's representations. Our approach hence gives a polynomial-size under-approximation in polynomial time.

ii) We further analyze the conservatism of this extended two-step approach. In particular, we show that any constrained zonotopic minuend has a "rich" enough CG-Rep, for which our two-step approach is exact. While it may be impractical to always assume such a rich CG-Rep, this result opens the direction of incrementally enriching the given CG-Rep of the minuend to improve the two-step approach's accuracy.

iii) Using the developed Minkowski difference technique, we propose two methods: scaling method and splitting method for BRS computation. The scaling method can compute BRSs with convex constraints for longer time horizon than the splitting method. In contrast, the splitting method can give larger BRSs than those obtained by scaling method for a short time horizon but have difficulties in computing BRSs for long time horizon. However, the splitting method can deal with nonconvex constraints and expand the BRSs into different homotopy classes. Experiments show the advantages of these constrained-zonotope-based methods: they give less conservative BRSs under-approximation than those using zonotopes [19], especially in the presence of state constraints, and scales better than the Hamilton-Jacobi (HJB) method [22].

II. Notations & Preliminaries

We use $\mathbf{1}$ ($\mathbf{0}$, resp.) to represent a matrix of proper size whose entries are all ones (zeros, resp.). We will not make the size of such a matrix explicit unless it is not clear from context. Let $\boldsymbol{M}$ be a matrix and $\boldsymbol{M}_1$ ($\boldsymbol{M}_2$, resp.) be another matrix of the same height (width, resp.) as $\boldsymbol{M}$, $[\boldsymbol{M}, \boldsymbol{M}_1]$ ($[\boldsymbol{M}; \boldsymbol{M}_2]$, resp.) denotes the matrix obtained by concatenating $\boldsymbol{M}$ and $\boldsymbol{M}_1$ horizontally (concatenating $\boldsymbol{M}$ and $\boldsymbol{M}_2$ vertically, resp.). Further, $\mathcal{N}(\boldsymbol{M})$ is the null space of $\boldsymbol{M}$ and $|\boldsymbol{M}|$ is the matrix that consists of the element-wise absolute values of $\boldsymbol{M}$.

Let $\underline{\boldsymbol{a}}$, $\overline{\boldsymbol{a}} \in \mathbb{R}^n$ such that $\underline{\boldsymbol{a}} \leq \overline{\boldsymbol{a}}$ ($\leq$ is element-wise), a *hyper-box* $[\![\underline{\boldsymbol{a}}, \overline{\boldsymbol{a}}]\!]$ is the set $\{\boldsymbol{x} \in \mathbb{R}^n \mid \underline{\boldsymbol{a}} \leq \boldsymbol{x} \leq \overline{\boldsymbol{a}}\}$. Let $\boldsymbol{G} \in \mathbb{R}^{n \times N}$ and $\boldsymbol{c} \in \mathbb{R}^n$, a *zonotope* $\mathcal{Z} = \langle \boldsymbol{G}, \boldsymbol{c} \rangle$ is defined to be the set $\{\boldsymbol{G\theta} + \boldsymbol{c} \mid \boldsymbol{\theta} \in [\![-\mathbf{1}, \mathbf{1}]\!]\}$. The tuple $\langle \boldsymbol{G}, \boldsymbol{c} \rangle$ is called the *generator-representation* (or G-Rep) of $\mathcal{Z}$. The matrix $\boldsymbol{G}$ is the *generator matrix* and $\boldsymbol{c}$ is the *center* of $\mathcal{Z}$. A set $\mathcal{CZ}$ is a *constrained zonotope* if it can be expressed as $\{\boldsymbol{G\theta} + \boldsymbol{c} \mid \boldsymbol{\theta} \in [\![-\mathbf{1}, \mathbf{1}]\!], \boldsymbol{A\theta} = \boldsymbol{b}\}$, where $\boldsymbol{A} \in \mathbb{R}^{m \times N}$ and $\boldsymbol{b} \in \mathbb{R}^m$. The tuple $\langle \boldsymbol{G}, \boldsymbol{c}, \boldsymbol{A}, \boldsymbol{b} \rangle$ is a *constrained generator representation* (or CG-Rep) of $\mathcal{CZ}$, $\boldsymbol{A}$ is the *constraint matrix* and $\boldsymbol{b}$ is the *constraint vector* of this CG-Rep. A zonotope $\langle \boldsymbol{G}, \boldsymbol{c} \rangle$ is a constrained zonotope whose CG-Rep has the same $\boldsymbol{G}$, $\boldsymbol{c}$ and empty $\boldsymbol{A}$, $\boldsymbol{b}$. Further, let $\boldsymbol{H} \in \mathbb{R}^{\ell \times N}$ and $\boldsymbol{a} \in \mathbb{R}^\ell$, a set is an *AH-polytope* if it can be expressed as $\{\boldsymbol{G\theta} + \boldsymbol{c} \mid \boldsymbol{H\theta} \leq \boldsymbol{a}\}$. Zonotopes and constrained zonotopes are AH-polytopes, i.e., $\langle \boldsymbol{G}, \boldsymbol{c} \rangle = \{\boldsymbol{G\theta} + \boldsymbol{c} \mid [\boldsymbol{I}; -\boldsymbol{I}]\boldsymbol{\theta} \leq \mathbf{1}\}$ and $\langle \boldsymbol{G}, \boldsymbol{c}, \boldsymbol{A}, \boldsymbol{b} \rangle = \{\boldsymbol{G\theta} + \boldsymbol{c} \mid [\boldsymbol{A}; -\boldsymbol{A}; \boldsymbol{I}; -\boldsymbol{I}]\boldsymbol{\theta} \leq [\boldsymbol{b}; -\boldsymbol{b}; \mathbf{1}]\}$.

Let $\mathcal{S}$, $\mathcal{R} \subseteq \mathbb{R}^n$ be two sets, $\boldsymbol{x} \in \mathbb{R}^n$ be a vector and $\boldsymbol{M} \in \mathbb{R}^{m \times n}$ be a matrix, we define $\boldsymbol{M}\mathcal{S} := \{\boldsymbol{Ms} \mid \boldsymbol{s} \in \mathcal{S}\}$ and $\boldsymbol{x} + \mathcal{S} := \{\boldsymbol{x} + \boldsymbol{s} \mid \boldsymbol{s} \in \mathcal{S}\}$. Further, $\mathcal{S} \oplus \mathcal{R} := \{\boldsymbol{s} + \boldsymbol{r} \mid \boldsymbol{s} \in \mathcal{S}, \boldsymbol{r} \in \mathcal{R}\}$ is the *Minkowski sum* of $\mathcal{S}$ and $\mathcal{R}$, and $\mathcal{S} \ominus \mathcal{R} := \{\boldsymbol{x} \in \mathbb{R}^n \mid \boldsymbol{x} + \mathcal{R} \subseteq \mathcal{S}\}$ is the *Minkowski difference* between $\mathcal{S}$ and $\mathcal{R}$. Let $\mathcal{P} \subseteq \mathbb{R}^p$, $\mathcal{S} \times \mathcal{P} := \{[\boldsymbol{s}; \boldsymbol{p}] \mid \boldsymbol{s} \in \mathcal{S}, \boldsymbol{p} \in \mathcal{P}\}$ is the *product* of $\mathcal{S}$ and $\mathcal{P}$.

The following set operations can be performed by CG-Rep manipulation for constrained zonotopes.

Lemma 1. [From [18], [21]] Let $\mathcal{CZ} = \langle \boldsymbol{G}, \boldsymbol{c}, \boldsymbol{A}, \boldsymbol{b} \rangle \subseteq \mathbb{R}^n$, $\mathcal{CZ}_i = \langle \boldsymbol{G}_i, \boldsymbol{c}_i, \boldsymbol{A}_i, \boldsymbol{b}_i \rangle \subseteq \mathbb{R}^p$ for $i \in \{1, 2\}$ be constrained zonotopes, $\boldsymbol{M} \in \mathbb{R}^{m \times n}$ be a matrix and $\mathcal{H} = \{\boldsymbol{x} \in \mathbb{R}^n \mid \boldsymbol{h}^\top \boldsymbol{x} \leq a\}$ be a halfspace, then

i) $\boldsymbol{M}\,\mathcal{CZ} = \langle \boldsymbol{MG}, \boldsymbol{Mc}, \boldsymbol{A}, \boldsymbol{b} \rangle$,
ii) $\mathcal{CZ}_1 \oplus \mathcal{CZ}_2 = \langle [\boldsymbol{G}_1, \boldsymbol{G}_2], \boldsymbol{c}_1 + \boldsymbol{c}_2, \mathrm{diag}(\boldsymbol{A}_1, \boldsymbol{A}_2), [\boldsymbol{b}_1; \boldsymbol{b}_2] \rangle$,
iii) $\mathcal{CZ}_1 \cap \mathcal{CZ}_2 = \langle [\boldsymbol{G}_1, \boldsymbol{0}], \boldsymbol{c}_1, [\mathrm{diag}(\boldsymbol{A}_1, \boldsymbol{A}_2); [\boldsymbol{G}_1, -\boldsymbol{G}_2]], [\boldsymbol{b}_1; \boldsymbol{b}_2; \boldsymbol{c}_2 - \boldsymbol{c}_1] \rangle$,
iv) if $\mathcal{CZ} \cap \mathcal{H} \neq \emptyset$, then $\mathcal{CZ} \cap \mathcal{H} = \langle [\boldsymbol{G}, \boldsymbol{0}], \boldsymbol{c}, [\boldsymbol{A}, \boldsymbol{0}; \boldsymbol{h}^\top \boldsymbol{G}, \frac{d}{2}], [\boldsymbol{b}; a - \boldsymbol{h}^\top \boldsymbol{c} - \frac{d}{2}] \rangle$ where $d = a - \boldsymbol{h}^\top \boldsymbol{c} + \|\boldsymbol{h}^\top \boldsymbol{G}\|_1$,
v) $\mathcal{CZ} \times \mathcal{CZ}_1 = \langle \mathrm{diag}(\boldsymbol{G}, \boldsymbol{G}_1), [\boldsymbol{c}; \boldsymbol{c}_1], \mathrm{diag}(\boldsymbol{A}, \boldsymbol{A}_1), [\boldsymbol{b}; \boldsymbol{b}_1] \rangle$.

The following lemma follows from the definitions.

Lemma 2. Let $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C} \subseteq \mathbb{R}^N$ and $\boldsymbol{M} \in \mathbb{R}^{n \times N}$

i) $\boldsymbol{M}(\mathcal{A} \oplus \mathcal{B}) = \boldsymbol{M}\mathcal{A} \oplus \boldsymbol{M}\mathcal{B}$.
ii) $\boldsymbol{M}(\mathcal{A} \ominus \mathcal{B}) \subseteq \boldsymbol{M}\mathcal{A} \ominus \boldsymbol{M}\mathcal{B}$.
iii) $(\mathcal{A} \ominus \mathcal{C}) \cup (\mathcal{B} \ominus \mathcal{C}) \subseteq (\mathcal{A} \cup \mathcal{B}) \ominus \mathcal{C}$.
iv) $\mathcal{A} \ominus \mathcal{B} \oplus \mathcal{C} \subseteq \mathcal{A} \oplus \mathcal{C} \ominus \mathcal{B}$.

For bullet ii), iii) and iv), equality does not hold in general.

Lemma 3. [[20], Theorem 1] Let $\mathcal{S}_i := \boldsymbol{c}_i + \boldsymbol{G}_i\{\boldsymbol{\theta}_i \mid \boldsymbol{H}_i\boldsymbol{\theta}_i \leq \boldsymbol{a}_i\} \subseteq \mathbb{R}^n$ for $i \in \{1, 2\}$ be two AH-polytopes. Suppose that $\mathcal{S}_1$ has nonempty interior. Then a sufficient condition for $\mathcal{S}_1 \subseteq \mathcal{S}_2$ is that there exist matrices $\boldsymbol{\Gamma}, \boldsymbol{\beta}, \boldsymbol{\Lambda}$ of proper sizes such that

$$\begin{aligned} &\boldsymbol{G}_1 = \boldsymbol{G}_2\boldsymbol{\Gamma},\ \boldsymbol{c}_2 - \boldsymbol{c}_1 = \boldsymbol{G}_2\boldsymbol{\beta},\ \boldsymbol{\Lambda}\boldsymbol{H}_1 = \boldsymbol{H}_2\boldsymbol{\Gamma}, \\ &\boldsymbol{\Lambda}\boldsymbol{a}_1 \leq \boldsymbol{a}_2 + \boldsymbol{H}_2\boldsymbol{\beta},\ \boldsymbol{\Lambda} \geq \boldsymbol{0}. \end{aligned} \tag{1}$$

The condition in Eq. (1) is known as the encoding of AH-polytope containment. The numbers of variables and constraints in Eq. (1) are polynomial in the sizes of $\boldsymbol{c}_i$, $\boldsymbol{G}_i$, $\boldsymbol{H}_i$, $\boldsymbol{a}_i$. Since the zonotope containment problem, which is a special instance of the AH-polytope containment problem, is known to be co-NP hard [23], the linear condition in Eq. (1) cannot possibly be necessary in general unless P = NP.

Lemma 4. [[14], Theorem 2.3] Let $\mathcal{S} \subseteq \mathbb{R}^n$ be compact, then $\{\boldsymbol{x} \mid \boldsymbol{H}\boldsymbol{x} \leq \boldsymbol{a}\} \ominus \mathcal{S} = \{x \mid \boldsymbol{H}\boldsymbol{x} \leq \underline{\boldsymbol{a}}\}$, where $\underline{a}_i = \max \boldsymbol{h}_i^\top \mathcal{S}$ is the i^{th} element of $\underline{\boldsymbol{a}}$ and $\boldsymbol{h}_i^\top$ is the i^{th} row of $\boldsymbol{H}$.

III. Problem Description

Consider the following discrete-time nonlinear system:

$$\boldsymbol{x}_{t+1} = \boldsymbol{f}(\boldsymbol{x}_t, \boldsymbol{u}_t) + \boldsymbol{w}_t, \tag{2}$$

where $\boldsymbol{x} \in \mathbb{R}^n$ is the state, $\boldsymbol{u} \in \mathcal{U} \subseteq \mathbb{R}^p$ is the control input, and $\boldsymbol{w} \in \mathcal{W} \subseteq \mathbb{R}^n$ is the additive disturbance input. Given a set $\mathcal{X}_{\text{safe}}$ of safe states and a set $\mathcal{X}_0$ of target states, the k^{th} backward reachable set $\mathcal{X}_k$ is defined recursively as follows:

$$\mathcal{X}_k = Pre(\mathcal{X}_{k-1}) := \begin{Bmatrix} \boldsymbol{x} \in \\ \mathcal{X}_{\text{safe}} \end{Bmatrix} \middle| \begin{array}{l} \exists \boldsymbol{u} \in \mathcal{U} : \forall \boldsymbol{w} \in \mathcal{W} : \\ \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{u}) + \boldsymbol{w} \in \mathcal{X}_{k-1} \end{array} \Bigg\}, \tag{3}$$

Our goal is to compute $\underline{\mathcal{X}}_k$, represented by constrained zonotopes, s.t. $\underline{\mathcal{X}}_k \subseteq \mathcal{X}_k$ under the following assumptions.

Assumption 1. The sets $\mathcal{X}_0, \mathcal{U}$ are constrained zonotopes (CG-Reps given). The disturbance set $\mathcal{W}$ is a zonotope (G-Rep given). The safe set $\mathcal{X}_{\text{safe}} = \bigcup_p \{\boldsymbol{x} \mid \boldsymbol{H}_p\boldsymbol{x} \leq \boldsymbol{a}_p\}$ is the union of finitely many polytopes in their H-Reps.

Our solution approach uses sequential linearization. If the system is linear, i.e., $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{u}) = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{B}\boldsymbol{u}$ for some invertible matrix $\boldsymbol{A}$ [1], then

$$\mathcal{X}_k = \mathcal{X}_{\text{safe}} \cap \boldsymbol{A}^{-1}(\mathcal{X}_{k-1} \ominus \mathcal{W} \oplus -\boldsymbol{B}\mathcal{U}). \tag{4}$$

For nonlinear systems, in each step, we linearize $\boldsymbol{f}$ at some $[\boldsymbol{x}^*; \boldsymbol{u}^*]$ and compute a under-approximation $\underline{\mathcal{X}}_k$ of $\mathcal{X}_k$ by applying Eq. (4) to the previously obtained $\underline{\mathcal{X}}_{k-1}$ and the linear dynamics. Particularly, to ensure that $\underline{\mathcal{X}}_{k-1}$ can be reached from $\underline{\mathcal{X}}_k$ under the nonlinear dynamics, we conservatively approximate the linearization error by an additive term that takes value from a zonotopic set $\mathcal{L}$, and require $\underline{\mathcal{X}}_{k-1} \ominus \mathcal{L}$ to be reachable from $\underline{\mathcal{X}}_k$ under the linear dynamics (i.e., replace $\mathcal{W}$ in Eq. (4) by $\mathcal{L} \oplus \mathcal{W}$).

The main challenge in the above approach is twofold:

C1) To implement Eq. (4) under Assumption 1, while the affine transformation, intersection and Minkowski addition can be done via CG-Rep manipulation (Lemma 1), there still lacks an efficient way to compute (or to under-approximate) the Minkowski difference between a constrained zonotopic minuend $\mathcal{X}_{k-1}$ and a zonotopic subtrahend $\mathcal{W}$ (or $\mathcal{L} \oplus \mathcal{W}$). Subsequent computations require this Minkowski difference to be in CG-Rep.
C2) To compute $\underline{\mathcal{X}}_k$, one needs to make a guess of $\mathcal{L}$ that encompasses all possible values of the additive linearization error over $\underline{\mathcal{X}}_k$, without knowing $\underline{\mathcal{X}}_k$ a priori.

The rest of the paper is devoted to tackling these two challenges. In Sec. IV, we develop an efficient algorithm for Minkowski difference under-approximation. We further show that our algorithm is exact for the problem instances whose minuend set has sufficiently rich CG-Reps (Sec. V). In Sec. VI, we explore two strategies to tackle challenge C2) and present two detailed algorithms that combine all ingredients together for BRS under-approximation.

IV. Under-approximating $\mathcal{CZ} \ominus \mathcal{Z}$

This section is concerned with under-approximating $\mathcal{CZ} \ominus \mathcal{Z}$, where $\mathcal{CZ} = \langle \boldsymbol{G}, \boldsymbol{c}, \boldsymbol{A}, \boldsymbol{b} \rangle \subseteq \mathbb{R}^n$ is a constrained zonotope and $\mathcal{Z} = \langle \boldsymbol{G}', \boldsymbol{c}' \rangle \subseteq \mathbb{R}^n$ is a zonotope. We will show that computing a compact CG-rep of the *exact* Minkowski difference is hard (Sec. IV-A). Hence we restrict our under-approximation to be a constrained zonotope $\mathcal{CZ}_{\text{d}}$ that shares the same "template" as the minuend $\mathcal{CZ}$, i.e., $\mathcal{CZ}_{\text{d}} = \langle \boldsymbol{G}\,\text{diag}(\overline{\boldsymbol{\delta}}), \boldsymbol{c}_{\text{d}}, \boldsymbol{A}\,\text{diag}(\overline{\boldsymbol{\delta}}), \boldsymbol{b}_{\text{d}} \rangle$ for some $\overline{\boldsymbol{\delta}} \in [\![\boldsymbol{0}, \boldsymbol{1}]\!]$, $\boldsymbol{c}_{\text{d}} \in \mathbb{R}^n$ and $\boldsymbol{b}_{\text{d}} \in \mathbb{R}^m$. Under such restrictions, one can enforce $\mathcal{CZ}_{\text{d}} \oplus \mathcal{Z} \subseteq \mathcal{CZ}$ using the constraints given by Lemma 3 and find $\mathcal{CZ}_{\text{d}}$ by solving an optimization problem. However, this optimization problem, as will be shown in Sec. IV-B, is a bilinear program. We refer to the above approach as the "naïve approach". To find a $\mathcal{CZ}_{\text{d}}$ more efficiently, in Sec. IV-C, we propose a two-step approach that amounts to solving a linear program. We further show how to reduce the size of this linear program and present some results to understand how conservative our under-approximation is.

A. Complexity Analysis

We show that, given the CG-Reps of $\mathcal{CZ}$ and $\mathcal{Z}$, it is impossible to find a polynomial-size CG-Rep of $\mathcal{CZ} \ominus \mathcal{Z}$ in polynomial time, unless P = NP. This motivates us to find an under-approximation that admits a polynomial-size CG-Rep computable in polynomial time.

Proposition 1. No algorithm satisfies the following two conditions simultaneously unless P = NP.

a) It finds $\langle \boldsymbol{G}'', \boldsymbol{c}'', \boldsymbol{A}'', \boldsymbol{b}'' \rangle = \mathcal{CZ} \ominus \mathcal{Z}$ in $\texttt{poly}(n, N, N')$ time, where N (N', resp.) is the width of $\boldsymbol{G}$ ($\boldsymbol{G}'$, resp.).
b) The widths and heights of matrices $\boldsymbol{G}'', \boldsymbol{c}'', \boldsymbol{A}'', \boldsymbol{b}''$ are $\texttt{poly}(n, N, N')$.

[1] The matrix $\boldsymbol{A}$ here is not to be confused with the constraint matrix in the CG-Rep of a constrained zonotope.

Proof: Assume that an algorithm A satisfies conditions a) and b) simultaneously. Since $\mathcal{Z} \subseteq \mathcal{CZ}$ iff $\mathbf{0} \in \mathcal{CZ} \ominus \mathcal{Z}$, whether $\mathcal{Z} \subseteq \mathcal{CZ}$ can be determined via the following procedure:
1) find $\langle \boldsymbol{G}'', \boldsymbol{c}'', \boldsymbol{A}'', \boldsymbol{b}'' \rangle$ by algorithm A,
2) claim $\mathcal{Z} \subseteq \mathcal{CZ}$ iff $\mathbf{0} \in \langle \boldsymbol{G}'', \boldsymbol{c}'', \boldsymbol{A}'', \boldsymbol{b}'' \rangle$.

By bullet a), step 1) takes $\texttt{poly}(n, N, N')$ time to run. Further, step 2) amounts to solving the following linear program:

$$\begin{array}{ll} \text{find} & \boldsymbol{\theta} \\ \text{s.t.} & \boldsymbol{G}''\boldsymbol{\theta} + \boldsymbol{c}'' = \mathbf{0},\ \boldsymbol{A}''\boldsymbol{\theta} = \boldsymbol{b}'',\ -\mathbf{1} \le \boldsymbol{\theta} \le \mathbf{1} \end{array} \tag{LP}$$

Let N'' (m'', resp.) be the width (height, resp.) of $\boldsymbol{A}''$, there are N'' variables and $2N''+m''+n$ constraints in (LP). These two numbers are $\texttt{poly}(n, N, N')$ by bullet b). Therefore, the above two-step procedure takes $\texttt{poly}(n, N, N')$ time to run. However, it is co-NP hard [23] to decide if $\mathcal{Z} \subseteq \mathcal{CZ}$ given the CG-Reps of $\mathcal{Z}$ and $\mathcal{CZ}$ as the inputs, which consist of $n(N+N'+2)$ reals. Hence the existence of such an algorithm A that satisfies a) and b) implies P = NP. ∎

B. Naïve Approach with Bilinear Constraints

With the aforementioned naïve approach, we need to solve the following optimization problem:

$$\begin{array}{ll} \max_{\overline{\boldsymbol{\delta}}, \boldsymbol{c}_\mathrm{d}, \boldsymbol{b}_\mathrm{d}} & \|\overline{\boldsymbol{\delta}}\|_1 \\ \text{s.t.} & \mathcal{CZ}_\mathrm{d} \oplus \mathcal{Z} \subseteq \mathcal{CZ} \end{array}. \tag{5}$$

The objective function $\|\overline{\boldsymbol{\delta}}\|_1$ is used as a heuristic to maximize the set $\mathcal{CZ}_\mathrm{d}$. To apply Lemma 3, we write $\mathcal{CZ}$ as an AH-polytope, i.e.,

$$\mathcal{CZ} = \boldsymbol{c} + \boldsymbol{G}\{\boldsymbol{\theta} \mid [\boldsymbol{A}; -\boldsymbol{A}; \boldsymbol{I}; -\boldsymbol{I}]\boldsymbol{\theta} \le [\boldsymbol{b}; -\boldsymbol{b}; \mathbf{1}]\}, \tag{6}$$

and write $\mathcal{CZ}_\mathrm{d} \oplus \mathcal{Z}$ either as

$$\begin{aligned} \boldsymbol{c}_\mathrm{d} + \boldsymbol{c}' + [\boldsymbol{G}\,\mathrm{diag}(\overline{\boldsymbol{\delta}}), \boldsymbol{G}']\{\boldsymbol{\xi} \mid [\boldsymbol{A}\,\mathrm{diag}(\overline{\boldsymbol{\delta}}), \mathbf{0}; \\ -\boldsymbol{A}\,\mathrm{diag}(\overline{\boldsymbol{\delta}}), \mathbf{0}; \boldsymbol{I}; -\boldsymbol{I}]\boldsymbol{\xi} \le [\boldsymbol{b}_\mathrm{d}; -\boldsymbol{b}_\mathrm{d}; \mathbf{1}]\}, \end{aligned} \tag{7}$$

or as

$$\begin{aligned} \boldsymbol{c}_\mathrm{d} + \boldsymbol{c}' + [\boldsymbol{G}, \boldsymbol{G}']\{\boldsymbol{\xi} \mid [\boldsymbol{A}, \mathbf{0}; -\boldsymbol{A}, \mathbf{0}; \boldsymbol{I}; -\boldsymbol{I}]\boldsymbol{\xi} \\ \le [\boldsymbol{b}_\mathrm{d}; -\boldsymbol{b}_\mathrm{d}; \overline{\boldsymbol{\delta}}; \mathbf{1}; \overline{\boldsymbol{\delta}}; \mathbf{1}]\}. \end{aligned} \tag{8}$$

Unfortunately, Lemma 3 gives bilinear constraints when applied to Eqs. (6),(7) or to Eqs. (6),(8). If (7) is used, "$\boldsymbol{H}_1$" in (1) depends on the variable $\overline{\boldsymbol{\delta}}$ and the term "$\boldsymbol{\Lambda}\boldsymbol{H}_1$" is bilinear; if (8) is used, "$\boldsymbol{a}_1$" in (1) depends on $\overline{\boldsymbol{\delta}}$ and "$\boldsymbol{\Lambda}\boldsymbol{a}_1$" is bilinear.

The key observation here is that the encoding in Lemma 3 is more favorable (i.e., tends to be linear) if the variables are related to the *outer* set. On the contrary, the above encoding is bilinear because the variable $\overline{\boldsymbol{\delta}}$ is related to the *inner* set.

C. Two-Step Approach: Overview

We propose an alternative approach that finds an under-approximation $\mathcal{CZ}_\mathrm{d}$ of $\mathcal{CZ} \ominus \mathcal{Z}$ with the following two steps.

I) Compute a vector $\overline{\boldsymbol{\sigma}} \in [\![\mathbf{0}, \mathbf{1}]\!]$ such that $\mathcal{CZ}_\mathrm{s} = \langle \boldsymbol{G}\,\mathrm{diag}(\overline{\boldsymbol{\sigma}}), \boldsymbol{c}_\mathrm{s}, A\,\mathrm{diag}(\overline{\boldsymbol{\sigma}}), \boldsymbol{b}_\mathrm{s} \rangle$ encloses $\mathcal{Z}$.
II) Compute $\mathcal{CZ}_\mathrm{d} = \langle \boldsymbol{G}\,\mathrm{diag}(\mathbf{1} - \overline{\boldsymbol{\sigma}}), \boldsymbol{c} - \boldsymbol{c}_\mathrm{s}, \boldsymbol{A}\,\mathrm{diag}(\mathbf{1} - \overline{\boldsymbol{\sigma}}), \boldsymbol{b} - \boldsymbol{b}_\mathrm{s} \rangle$.

Since $\mathcal{Z} \subseteq \mathcal{CZ}_\mathrm{s}$ by construction, $\mathcal{CZ} \ominus \mathcal{CZ}_\mathrm{s}$ is an under-approximation of $\mathcal{CZ} \ominus \mathcal{Z}$. The significance of Step I) is that, since the variable $\overline{\boldsymbol{\sigma}}$ is related to the *outer* set $\mathcal{CZ}_\mathrm{s}$, the encoding of $\mathcal{Z} \subseteq \mathcal{CZ}_\mathrm{s}$ by Lemma 3 is linear. Further, since the generator matrix $\boldsymbol{G}$ and the constraint matrix $\boldsymbol{A}$ of the minuend $\mathcal{CZ}$ are used as "templates" when constructing $\mathcal{CZ}_\mathrm{s}$, it follows that $\mathcal{CZ} \ominus \mathcal{CZ}_\mathrm{s} \supseteq \mathcal{CZ}_\mathrm{d} = \langle \boldsymbol{G}\,\mathrm{diag}(\mathbf{1} - \overline{\boldsymbol{\sigma}}), \boldsymbol{c} - \boldsymbol{c}_\mathrm{s}, \boldsymbol{A}\,\mathrm{diag}(\mathbf{1} - \overline{\boldsymbol{\sigma}}), \boldsymbol{b} - \boldsymbol{b}_\mathrm{s} \rangle$. Hence $\mathcal{CZ} \ominus \mathcal{CZ}_\mathrm{s}$ can be further under-approximated via a simple CG-Rep manipulation. The above two-step approach extends the one in [19] for under-approximating the Minkowski difference of two zonotopes.

In what follows, we first show in details how to implement Step I) by solving a linear program. We further simplify this linear program by showing that it is optimal to choose $\boldsymbol{c}_\mathrm{s} = \boldsymbol{c}'$ and $\boldsymbol{b}_\mathrm{s} = \mathbf{0}$ in Step I). Then we prove that $\mathcal{CZ} \ominus \mathcal{CZ}_\mathrm{s} \supseteq \mathcal{CZ}_\mathrm{d}$. As a step to understand the conservatism of our under-approximation, we will also give a sufficient condition for $\mathcal{CZ} \ominus \mathcal{CZ}_\mathrm{s} = \mathcal{CZ}_\mathrm{d}$ to hold.

D. Step I: Over-approximating $\mathcal{Z}$ by $\mathcal{CZ}_\mathrm{s}$

Our goal is to solve

$$\begin{array}{ll} \min_{\overline{\boldsymbol{\sigma}}, \boldsymbol{c}_\mathrm{s}, \boldsymbol{b}_\mathrm{s}} & \|\overline{\boldsymbol{\sigma}}\|_1 \\ \text{s.t.} & \mathcal{Z} \subseteq \mathcal{CZ}_\mathrm{s} \end{array}, \tag{9}$$

where $\mathcal{Z} = \langle \boldsymbol{G}', \boldsymbol{c}' \rangle$ and $\mathcal{CZ}_\mathrm{s} = \langle \boldsymbol{G}\,\mathrm{diag}(\overline{\boldsymbol{\sigma}}), \boldsymbol{c}_\mathrm{s}, \boldsymbol{A}\,\mathrm{diag}(\overline{\boldsymbol{\sigma}}), \boldsymbol{b}_\mathrm{s} \rangle$. In (9), we minimize $\|\overline{\boldsymbol{\sigma}}\|_1$. This can be seen as a heuristic to minimize the enclosing constrained zonotope $\mathcal{CZ}_\mathrm{s}$. Note that $\mathcal{CZ}_\mathrm{s}$ can be rewritten as $\boldsymbol{c}_\mathrm{s} + \boldsymbol{G}\mathcal{S}_{\boldsymbol{b}_\mathrm{s}}$ where $\mathcal{S}_{\boldsymbol{b}_\mathrm{s}} = \{\boldsymbol{\sigma} \in [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!] \mid \boldsymbol{A}\boldsymbol{\sigma} = \boldsymbol{b}_\mathrm{s}\}$.

The following result shows that, to solve the optimization problem in (9), one can choose $\boldsymbol{c}_\mathrm{s} = \boldsymbol{c}'$ and $\boldsymbol{b}_\mathrm{s} = \mathbf{0}$ without loss of optimality.

Proposition 2. Let $\mathcal{S}_{\boldsymbol{b}_\mathrm{s}} := \{\boldsymbol{\sigma} \in [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!] \mid \boldsymbol{A}\boldsymbol{\sigma} = \boldsymbol{b}_\mathrm{s}\}$ and $\mathcal{Z}$ be a zonotope centering at $\boldsymbol{c}'$. We have

$$\begin{aligned} & \min\{\|\overline{\boldsymbol{\sigma}}\|_1 \mid \mathcal{Z} \subseteq \boldsymbol{c}' + \boldsymbol{G}\mathcal{S}_{\mathbf{0}}\} \\ \le\ & \min\{\|\overline{\boldsymbol{\sigma}}\|_1 \mid \exists \boldsymbol{c}_\mathrm{s}, \boldsymbol{b}_\mathrm{s} : \mathcal{Z} \subseteq \boldsymbol{c}_\mathrm{s} + \boldsymbol{G}\mathcal{S}_{\boldsymbol{b}_\mathrm{s}}\}. \end{aligned} \tag{10}$$

Proof: We first prove that $\mathcal{Z} \subseteq \boldsymbol{c}_\mathrm{s} + \boldsymbol{G}\,\mathcal{S}_{\boldsymbol{b}_\mathrm{s}}$ implies $\mathcal{Z} \subseteq \boldsymbol{c}' + \boldsymbol{G}\mathcal{S}_{\mathbf{0}}$. Note that $\mathcal{Z}$ is symmetric w.r.t its center $\boldsymbol{c}'$, i.e., $-\mathcal{Z} + \boldsymbol{c}' = \mathcal{Z} - \boldsymbol{c}'$. By $\mathcal{Z} \subseteq \boldsymbol{c}_\mathrm{s} + \boldsymbol{G}\,\mathcal{S}_{\boldsymbol{b}_\mathrm{s}}$, we have

$$\begin{aligned} & \mathcal{Z} - \boldsymbol{c}' \\ \subseteq\ & (\boldsymbol{c}_\mathrm{s} - \boldsymbol{c}') + \boldsymbol{G}\,\mathcal{S}_{\boldsymbol{b}_\mathrm{s}} \cap -(\boldsymbol{c}_\mathrm{s} - \boldsymbol{c}') - \boldsymbol{G}\,\mathcal{S}_{\boldsymbol{b}_\mathrm{s}} \\ =\ & \left\{ \begin{array}{c|l} \boldsymbol{G}\boldsymbol{\theta} + & \boldsymbol{\theta}, \boldsymbol{\mu} \in [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!], \boldsymbol{A}\boldsymbol{\theta} = \boldsymbol{A}\boldsymbol{\mu} = \boldsymbol{b}_\mathrm{s}, \\ (\boldsymbol{c}_\mathrm{s} - \boldsymbol{c}') & \boldsymbol{G}\boldsymbol{\theta} + (\boldsymbol{c}_\mathrm{s} - \boldsymbol{c}') = -\boldsymbol{G}\boldsymbol{\mu} - (\boldsymbol{c}_\mathrm{s} - \boldsymbol{c}') \end{array} \right\} \\ \subseteq\ & \left\{ \boldsymbol{G}\boldsymbol{\theta} - \boldsymbol{G}\left(\tfrac{\boldsymbol{\mu}+\boldsymbol{\theta}}{2}\right) \,\middle|\, \boldsymbol{\theta}, \boldsymbol{\mu} \in [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!], \boldsymbol{A}(\boldsymbol{\theta} - \boldsymbol{\mu}) = \mathbf{0} \right\} \\ =\ & \left\{ \boldsymbol{G}\left(\tfrac{\boldsymbol{\theta}-\boldsymbol{\mu}}{2}\right) \,\middle|\, \tfrac{\boldsymbol{\theta}-\boldsymbol{\mu}}{2} \in [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!], \boldsymbol{A}\left(\tfrac{\boldsymbol{\theta}-\boldsymbol{\mu}}{2}\right) = \mathbf{0} \right\} \\ =\ & \{\boldsymbol{G}\boldsymbol{\sigma} \mid \boldsymbol{\sigma} \in [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!], \boldsymbol{A}\boldsymbol{\sigma} = \mathbf{0}\} = G\mathcal{S}_{\mathbf{0}} \end{aligned} \tag{11}$$

Therefore, we have $\mathcal{Z} \subseteq \boldsymbol{c}' + G\mathcal{S}_{\mathbf{0}}$. Since $\mathcal{S}_{\boldsymbol{b}_\mathrm{s}}$ and $\mathcal{S}_{\mathbf{0}}$ are defined by the same $\overline{\boldsymbol{\sigma}}$, Eq. (10) follows readily. ∎

Remark 1. Proposition 2 holds for any set $\mathcal{Z}$ that is symmetric w.r.t. $\boldsymbol{c}'$ and any other cost function of $\overline{\boldsymbol{\sigma}}$ than $\|\overline{\boldsymbol{\sigma}}\|_1$.

Next, we show that, with the sufficient condition for $\mathcal{Z} \subseteq \mathcal{CZ}_\mathrm{s}$ given in Lemma 3, how to find a suboptimal solution of (9) by solving a linear program.

Proposition 3. Suppose that $\mathcal{Z} = \langle \boldsymbol{G}', \boldsymbol{c}' \rangle$ has nonempty interior. Let $\overline{\boldsymbol{\sigma}}$ be part of a minimizer of the following linear program:

$$\begin{aligned} \min_{\overline{\boldsymbol{\sigma}}, \boldsymbol{c}_\mathrm{s}, \boldsymbol{b}_\mathrm{s}, \boldsymbol{\Gamma}, \boldsymbol{\beta}, \boldsymbol{\Lambda}} \quad & \|\overline{\boldsymbol{\sigma}}\|_1 \\ \text{s.t.} \quad & \boldsymbol{G}' = \boldsymbol{G}\boldsymbol{\Gamma}, \boldsymbol{G}\boldsymbol{\beta} = \boldsymbol{c}_\mathrm{s} - \boldsymbol{c}', \\ & \boldsymbol{\Lambda}[\boldsymbol{I}; -\boldsymbol{I}] = [\boldsymbol{A}; -\boldsymbol{A}; \boldsymbol{I}; -\boldsymbol{I}]\boldsymbol{\Gamma}, \\ & \boldsymbol{\Lambda}\boldsymbol{1} \leq [\boldsymbol{b}_\mathrm{s}; -\boldsymbol{b}_\mathrm{s}; \overline{\boldsymbol{\sigma}}; \overline{\boldsymbol{\sigma}}] + [\boldsymbol{A}; -\boldsymbol{A}; \boldsymbol{I}; -\boldsymbol{I}]\boldsymbol{\beta}, \\ & \boldsymbol{0} \leq \overline{\boldsymbol{\sigma}} \leq \boldsymbol{1}, \ \boldsymbol{\Lambda} \geq \boldsymbol{0} \end{aligned} \tag{min-out}$$

then $\mathcal{Z} \subseteq \mathcal{CZ}_\mathrm{s} = \langle G\,\mathrm{diag}(\overline{\boldsymbol{\sigma}}), \boldsymbol{c}_\mathrm{s}, A\,\mathrm{diag}(\overline{\boldsymbol{\sigma}}), \boldsymbol{b}_\mathrm{s} \rangle$.

Proof: Note that the constrained zonotope $\mathcal{CZ}_\mathrm{s}$ and the zonotope $\mathcal{Z}$ can be written as

$$\mathcal{CZ}_\mathrm{s} = \boldsymbol{c}_\mathrm{s} + \boldsymbol{G}\{\boldsymbol{\sigma} \mid [\boldsymbol{A}; -\boldsymbol{A}; \boldsymbol{I}; -\boldsymbol{I}]\boldsymbol{\sigma} \leq [\boldsymbol{b}_\mathrm{s}; -\boldsymbol{b}_\mathrm{s}; \overline{\boldsymbol{\sigma}}; \overline{\boldsymbol{\sigma}}]\}, \tag{12}$$

$$\mathcal{Z} = \boldsymbol{c}' + \boldsymbol{G}'\{\boldsymbol{\sigma} \mid [\boldsymbol{I}; -\boldsymbol{I}]\boldsymbol{\sigma} \leq \boldsymbol{1}\}. \tag{13}$$

Therefore $\mathcal{CZ}_\mathrm{s} \supseteq \mathcal{Z}$ can be enforced by a set of linear constraints using Lemma 3, which leads to (min-out). ■

In spite of Proposition 2, we keep $\boldsymbol{c}_\mathrm{s}$, $\boldsymbol{b}_\mathrm{s}$ as free variables in (min-out). In what follows, we show that one can also set $\boldsymbol{c}_\mathrm{s} = \boldsymbol{c}'$ and $\boldsymbol{b}_\mathrm{s} = \boldsymbol{0}$ in (min-out) without loss of optimality. This result leads to a linear program equivalent to (min-out) with fewer variables and constraints. Note that this result does not follow immediately from Proposition 2 because the condition in Lemma 3 is only sufficient but not necessary in general (in fact, if that condition were also necessary, it would be straightforward that $\boldsymbol{c}_\mathrm{s} = \boldsymbol{c}'$ and $\boldsymbol{b}_\mathrm{s} = \boldsymbol{0}$ is optimal for (min-out)). The proof is based on the following observations.

Proposition 4. Let $(\overline{\boldsymbol{\sigma}}, \boldsymbol{c}_\mathrm{s}, \boldsymbol{b}_\mathrm{s}, \boldsymbol{\Gamma}, \boldsymbol{\beta}, \boldsymbol{\Lambda})$ be a feasible solution of (min-out), then i) $\boldsymbol{c}_\mathrm{s} = \boldsymbol{G}\boldsymbol{\beta} - \boldsymbol{c}'$, ii) $\boldsymbol{b}_\mathrm{s} = -\boldsymbol{A}\boldsymbol{\beta}$ and iii) $\boldsymbol{A}\boldsymbol{\Gamma} = \boldsymbol{0}$, and iv) $(\overline{\boldsymbol{\sigma}}, \boldsymbol{c}', \boldsymbol{0}, \boldsymbol{\Gamma}, \boldsymbol{0}, \underline{\boldsymbol{\Lambda}})$ is feasible for some $\underline{\boldsymbol{\Lambda}}$.

Proof: Bullet i) follows from the constraint $\boldsymbol{G}\boldsymbol{\beta} = \boldsymbol{c}_\mathrm{s} - \boldsymbol{c}'$. By $\boldsymbol{\Lambda} \geq \boldsymbol{0}$ (hence $\boldsymbol{\Lambda}\boldsymbol{1} \geq \boldsymbol{0}$) and $\boldsymbol{\Lambda}\boldsymbol{1} \leq [\boldsymbol{b}_\mathrm{s}; -\boldsymbol{b}_\mathrm{s}; \overline{\boldsymbol{\sigma}}; \overline{\boldsymbol{\sigma}}] + [\boldsymbol{A}; -\boldsymbol{A}; \boldsymbol{I}; -\boldsymbol{I}]\boldsymbol{\beta}$, we have

$$\boldsymbol{0} \leq \boldsymbol{\Lambda}\boldsymbol{1} \leq [\boldsymbol{b}_\mathrm{s}; -\boldsymbol{b}_\mathrm{s}; \overline{\boldsymbol{\sigma}}; \overline{\boldsymbol{\sigma}}] + [\boldsymbol{A}; -\boldsymbol{A}; \boldsymbol{I}; -\boldsymbol{I}]\boldsymbol{\beta}. \tag{14}$$

This implies that $\boldsymbol{0} \leq \boldsymbol{b}_\mathrm{s} + \boldsymbol{A}\boldsymbol{\beta}$ and $\boldsymbol{0} \leq -\boldsymbol{b}_\mathrm{s} - \boldsymbol{A}\boldsymbol{\beta}$, i.e., $\boldsymbol{b}_\mathrm{s} + \boldsymbol{A}\boldsymbol{\beta} = \boldsymbol{0}$. Hence bullet ii) holds. Also, $\boldsymbol{\Lambda}\boldsymbol{1} = [\boldsymbol{0}_{2m}; \overline{\boldsymbol{\sigma}} + \boldsymbol{\beta}; \overline{\boldsymbol{\sigma}} - \boldsymbol{\beta}]$ and hence the upper part of matrix $\boldsymbol{\Lambda}$ must be all zeros, i.e., $\boldsymbol{\Lambda} = [\boldsymbol{0}_{2m \times 2N'}; \tilde{\boldsymbol{\Lambda}}]$ for some $\tilde{\boldsymbol{\Lambda}} \geq \boldsymbol{0}$, where m is the height of $\boldsymbol{A}$ and N' is the width of $\boldsymbol{G}'$. This further implies that $\boldsymbol{A}\boldsymbol{\Gamma} = \boldsymbol{0}$ because $\boldsymbol{\Lambda}[\boldsymbol{I}; -\boldsymbol{I}] = [\boldsymbol{A}; -\boldsymbol{A}; \boldsymbol{I}; -\boldsymbol{I}]\boldsymbol{\Gamma}$.

To prove bullet iv), define $\underline{\boldsymbol{\Lambda}}$ as follows. The topmost $2m$ rows of $\underline{\boldsymbol{\Lambda}}$ are all zeros. For $i = 1, 2 \ldots N$, where N is the width of $\boldsymbol{G}$,

i) if the i^{th} element of $\boldsymbol{\beta}$ is non-positive, define the $2m + i^{\text{th}}$ row of $\underline{\boldsymbol{\Lambda}}$ to be the same as that of $\boldsymbol{\Lambda}$, i.e., $[\boldsymbol{\Lambda}_{2m+i,1:N'}, \boldsymbol{\Lambda}_{2m+i,N'+1:2N'}]$, and the $2m+N+i^{\text{th}}$ row of $\underline{\boldsymbol{\Lambda}}$ to be $[\boldsymbol{\Lambda}_{2m+i,N'+1:2N'}, \boldsymbol{\Lambda}_{2m+i,1:N'}]$;
ii) if the i^{th} element of $\boldsymbol{\beta}$ is positive, define the $2m + N + i^{\text{th}}$ row of $\underline{\boldsymbol{\Lambda}}$ to be the same as that of $\boldsymbol{\Lambda}$, i.e., $[\boldsymbol{\Lambda}_{2m+N+i,1:N'}, \boldsymbol{\Lambda}_{2m+N+i,N'+1:2N'}]$, and the $2m + i^{\text{th}}$ row of $\underline{\boldsymbol{\Lambda}}$ to be $[\boldsymbol{\Lambda}_{2m+N+i,N'+1:2N'}, \boldsymbol{\Lambda}_{2m+N+i,1:N'}]$.

By construction, $\underline{\boldsymbol{\Lambda}}$ has a special structure, i.e., $\underline{\boldsymbol{\Lambda}} = [\boldsymbol{0}_{2m \times 2N'}; \boldsymbol{\Lambda}_1, \boldsymbol{\Lambda}_2; \boldsymbol{\Lambda}_2, \boldsymbol{\Lambda}_1]$. Moreover, $\underline{\boldsymbol{\Lambda}}[\boldsymbol{I}; -\boldsymbol{I}] = [\boldsymbol{0}_{2m}; \boldsymbol{\Gamma}; -\boldsymbol{\Gamma}]$ and that $\underline{\boldsymbol{\Lambda}}\boldsymbol{1} \leq [\boldsymbol{0}_{2m}; \overline{\boldsymbol{\sigma}} - |\boldsymbol{\beta}|; \overline{\boldsymbol{\sigma}} - |\boldsymbol{\beta}|] \leq [\boldsymbol{0}_{2m}; \overline{\boldsymbol{\sigma}}; \overline{\boldsymbol{\sigma}}]$. Together with bullet i) ii) and iii), it is straightforward to check that $(\overline{\boldsymbol{\sigma}}, \boldsymbol{c}', \boldsymbol{0}, \boldsymbol{\Gamma}, \boldsymbol{0}, \underline{\boldsymbol{\Lambda}})$ is feasible. ■

Proposition 4 leads to a simplification of (min-out).

Theorem 1. The linear program (min-out) is equivalent to

$$\begin{aligned} \min_{\boldsymbol{\Gamma}} \quad & \||\boldsymbol{\Gamma}|\boldsymbol{1}\|_1 \\ \text{s.t.} \quad & [\boldsymbol{G}; \boldsymbol{A}]\boldsymbol{\Gamma} = [\boldsymbol{G}'; \boldsymbol{0}], \ |\boldsymbol{\Gamma}|\boldsymbol{1} \leq \boldsymbol{1} \end{aligned}. \tag{simple}$$

Proof: If $\boldsymbol{\Gamma}$ minimizes (simple), $(\overline{\boldsymbol{\sigma}}, \boldsymbol{c}', \boldsymbol{0}, \boldsymbol{\Gamma}, \boldsymbol{0}, \underline{\boldsymbol{\Lambda}})$ is feasible to (min-out), where $\overline{\boldsymbol{\sigma}} = |\boldsymbol{\Gamma}|\boldsymbol{1}$, $\underline{\boldsymbol{\Lambda}} = [\boldsymbol{0}_{2m \times 2N'}; \boldsymbol{\Lambda}_1, \boldsymbol{\Lambda}_2; \boldsymbol{\Lambda}_2, \boldsymbol{\Lambda}_1]$, $\boldsymbol{\Lambda}_1 = \boldsymbol{\Gamma}^+ := (|\boldsymbol{\Gamma}| + \boldsymbol{\Gamma})/2$ and $\boldsymbol{\Lambda}_2 = \boldsymbol{\Gamma}^- := (|\boldsymbol{\Gamma}| - \boldsymbol{\Gamma})/2$. Moreover, the cost given by this feasible solution is $\|\overline{\boldsymbol{\sigma}}\|_1 = \||\boldsymbol{\Gamma}|\boldsymbol{1}\|_1$, i.e., the same as the minimum of (simple).

Suppose that $(\overline{\boldsymbol{\sigma}}, \boldsymbol{c}_\mathrm{s}, \boldsymbol{b}_\mathrm{s}, \boldsymbol{\Gamma}, \boldsymbol{\beta}, \boldsymbol{\Lambda})$ minimizes (min-out). Construct $\underline{\boldsymbol{\Lambda}}$ from $\boldsymbol{\Lambda}$ as in the proof of Proposition 4, and let $[\boldsymbol{\Lambda}_1, \boldsymbol{\Lambda}_2]$ consist of the $2m + 1^{\text{st}}$ to $2m + N^{\text{th}}$ rows of $\underline{\boldsymbol{\Lambda}}$. Then $\boldsymbol{\Gamma} = \boldsymbol{\Lambda}_1 - \boldsymbol{\Lambda}_2$ is feasible to (simple). Further, the cost associated with $\boldsymbol{\Gamma}$ is $\||\boldsymbol{\Gamma}|\boldsymbol{1}\|_1 \leq \|\overline{\boldsymbol{\sigma}}\|_1$. This is because, by Proposition 4, $(\overline{\boldsymbol{\sigma}}, \boldsymbol{c}', \boldsymbol{0}, \boldsymbol{\Gamma}, \boldsymbol{0}, \underline{\boldsymbol{\Lambda}})$ is also feasible to (min-out) and hence $\overline{\boldsymbol{\sigma}} \geq \boldsymbol{\Lambda}_1\boldsymbol{1} + \boldsymbol{\Lambda}_2\boldsymbol{1} = |\boldsymbol{\Gamma}|\boldsymbol{1}$ must hold. ■

By Theorem 1, we can find the minimizer $\boldsymbol{\Gamma}$ of (simple), define $\overline{\boldsymbol{\sigma}} = |\boldsymbol{\Gamma}|\boldsymbol{1}$ and $\langle \boldsymbol{G}\,\mathrm{diag}(\overline{\boldsymbol{\sigma}}), \ \boldsymbol{c}', \boldsymbol{A}\,\mathrm{diag}(\overline{\boldsymbol{\sigma}}), \boldsymbol{0} \rangle$ is guaranteed to enclose $\mathcal{Z}$. From now no, we will use $\mathcal{CZ}_\mathrm{s}$ to denote the constrained zonotope $\langle \boldsymbol{G}\,\mathrm{diag}(\overline{\boldsymbol{\sigma}}), \boldsymbol{c}', \boldsymbol{A}\,\mathrm{diag}(\overline{\boldsymbol{\sigma}}), \boldsymbol{0} \rangle$ and omit the subscript "$\boldsymbol{0}$" of the set $\mathcal{S}_\mathbf{0} = \{\boldsymbol{\sigma} \in [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!] \mid \boldsymbol{A}\boldsymbol{\sigma} = \boldsymbol{0}\}$.

The simplified optimization problem (simple) has a geometric interpretation. Its decision variable $\boldsymbol{\Gamma}$ can be viewed as the generator matrix of a zonotope $\langle \boldsymbol{\Gamma}, \boldsymbol{0} \rangle \subseteq \mathbb{R}^N$, where N is the width of $\boldsymbol{G}$. The inner zonotope $\mathcal{Z}$ is the image of $\langle \boldsymbol{\Gamma}, \boldsymbol{0} \rangle$ under linear map $\boldsymbol{G}$ and translation $\boldsymbol{c}'$. Moreover, $\langle \boldsymbol{\Gamma}, \boldsymbol{0} \rangle$ is in the null space of $\boldsymbol{A}$, and $[\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!]$ is the smallest hyper-box that encloses $\langle \boldsymbol{\Gamma}, \boldsymbol{0} \rangle$ as $\overline{\boldsymbol{\sigma}} = |\boldsymbol{\Gamma}|\boldsymbol{1}$. With this interpretation, it is easy to see $\mathcal{Z} \subseteq \mathcal{CZ}_\mathrm{s}$. To be precise,

$$\begin{aligned} \mathcal{Z} &= \langle \boldsymbol{G}', \boldsymbol{c}' \rangle \\ &= \{\boldsymbol{G}\boldsymbol{\Gamma}\boldsymbol{\theta} + \boldsymbol{c}' \mid \boldsymbol{\theta} \in [\![-\boldsymbol{1}, \boldsymbol{1}]\!]\} && (\boldsymbol{G}\boldsymbol{\Gamma} = \boldsymbol{G}') \\ &= \{\boldsymbol{G}\boldsymbol{\sigma} + \boldsymbol{c}' \mid \boldsymbol{\sigma} \in \langle \boldsymbol{\Gamma}, \boldsymbol{0} \rangle\} \\ &= \{\boldsymbol{G}\boldsymbol{\sigma} + \boldsymbol{c}' \mid \boldsymbol{\sigma} \in \langle \boldsymbol{\Gamma}, \boldsymbol{0} \rangle, \boldsymbol{A}\boldsymbol{\sigma} = \boldsymbol{0}\} && (\boldsymbol{A}\boldsymbol{\Gamma} = \boldsymbol{0}) \\ &\subseteq \{\boldsymbol{G}\boldsymbol{\sigma} + \boldsymbol{c}' \mid \boldsymbol{\sigma} \in [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!], \boldsymbol{A}\boldsymbol{\sigma} = \boldsymbol{0}\} && (\overline{\boldsymbol{\sigma}} = |\boldsymbol{\Gamma}|\boldsymbol{1}) \\ &= \boldsymbol{c}' + \boldsymbol{G}\mathcal{S} = \mathcal{CZ}_\mathrm{s}. \end{aligned} \tag{15}$$

Remark 2. For arbitrary constrained zonotope $\langle \boldsymbol{G}, \boldsymbol{c}, \boldsymbol{A}, \boldsymbol{b} \rangle$, the unit hyper-box $[\![-\boldsymbol{1}, \boldsymbol{1}]\!]$ may not necessarily be *tight*, i.e., it is not the smallest hyper-box that encloses $\{\boldsymbol{\theta} \in [\![-\boldsymbol{1}, \boldsymbol{1}]\!] \mid \boldsymbol{A}\boldsymbol{\theta} = \boldsymbol{b}\}$. Such a tight hyper-box can be founded by solving $2N$ linear programs, where N is the width of matrix $\boldsymbol{G}$, or can be outer-approximated more efficiently by an iterative method proposed in [21]. However, for $\langle \boldsymbol{G}\,\mathrm{diag}(\overline{\boldsymbol{\sigma}}), \boldsymbol{c}', \boldsymbol{A}\,\mathrm{diag}(\overline{\boldsymbol{\sigma}}), \boldsymbol{0} \rangle$ obtained by solving (simple), $[\![-\boldsymbol{1}, \boldsymbol{1}]\!]$ is tight. This is because, by the above interpretation, $[\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!]$ is the smallest hyper-box

that contains $\langle \boldsymbol{\Gamma}, \mathbf{0} \rangle \subseteq \{\boldsymbol{\sigma} \in [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!] \mid \boldsymbol{A}\boldsymbol{\sigma} = \mathbf{0}\} = \mathcal{S}$. Hence $[\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!]$ is also the smallest hyper-box containing $\mathcal{S}$. As we will see, the tightness of $[\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!]$ plays an important role in the conservatism analysis of Step II.

Remark 3. The cost function $\||\boldsymbol{\Gamma}|\mathbf{1}\|_1$ of (simple) is the absolute element sum of the matrix $\boldsymbol{\Gamma}$. One may ask whether minimizing this cost would achieve $|\boldsymbol{\Gamma}|\mathbf{1} \leq \mathbf{1}$ whenever possible, even after removing the constraint $|\boldsymbol{\Gamma}|\mathbf{1} \leq \mathbf{1}$. This is not the case in general though it happens often times. If we ignore $|\boldsymbol{\Gamma}|\mathbf{1} \leq \mathbf{1}$ in (simple) and minimize the Frobenius norm of $\boldsymbol{\Gamma}$ instead, it is equivalent to finding the minimum norm solution of the least square problem defined by $[\boldsymbol{G}; \boldsymbol{A}]\boldsymbol{\Gamma} = [\boldsymbol{G}'; \mathbf{0}]$. If this minimum norm solution also satisfies $|\boldsymbol{\Gamma}|\mathbf{1} \leq \mathbf{1}$, then it is a good estimate of the minimizer of (min-out) and can be found more efficiently.

E. Step II: $\mathcal{CZ} \ominus \mathcal{CZ}_\mathrm{s}$ by CG-Rep Manipulation

We further under-approximate $\mathcal{CZ} \ominus \mathcal{CZ}_\mathrm{s}$ by $\mathcal{CZ}_\mathrm{d} = \langle \boldsymbol{G}\,\mathrm{diag}(\mathbf{1} - \overline{\boldsymbol{\sigma}}), \boldsymbol{c} - \boldsymbol{c}', \boldsymbol{A}\,\mathrm{diag}(\mathbf{1} - \overline{\boldsymbol{\sigma}}), \boldsymbol{b} \rangle$. It is tempting to conclude that $\mathcal{CZ}_\mathrm{d} = \mathcal{CZ} \ominus \mathcal{CZ}_\mathrm{s}$, but this is not true in general. In what follows, we show $\mathcal{CZ}_\mathrm{d} \subseteq \mathcal{CZ} \ominus \mathcal{CZ}_\mathrm{s}$ and give a sufficient condition for this under-approximation to be exact.

The following two propositions will be useful later.

Proposition 5. Define

$$\mathcal{M} = \{\boldsymbol{\mu} \in [\![-\overline{\boldsymbol{\delta}}, \overline{\boldsymbol{\delta}}]\!] \oplus [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!] \mid \boldsymbol{A}\boldsymbol{\mu} = \boldsymbol{b}\}, \tag{16}$$

$$\mathcal{S} = \{\sigma \in [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!] \mid \boldsymbol{A}\boldsymbol{\sigma} = \mathbf{0}\}, \tag{17}$$

$$\mathcal{D} = \{\boldsymbol{\delta} \in [\![-\overline{\boldsymbol{\delta}}, \overline{\boldsymbol{\delta}}]\!] \mid \boldsymbol{A}\boldsymbol{\delta} = \boldsymbol{b}\}. \tag{18}$$

Assume that $[\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!]$ is the smallest hyper-box that contains $\mathcal{S}$. Then $\mathcal{M} \ominus \mathcal{S} = \mathcal{D}$.

Proof: This is a direct result of Lemma 4. Particularly, since $[\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!]$ is the smallest hyper-box that contains $\mathcal{S}$, $\max \pm \boldsymbol{e}_i^\top \mathcal{S} = \pm\overline{\sigma}_i$, where $\boldsymbol{e}_i$ is the i^{th} natural basis vector and $\overline{\sigma}_i$ is the i^{th} element of $\overline{\boldsymbol{\sigma}}$. ■

Proposition 6. Define $\mathcal{M}, \mathcal{S} \subseteq \mathbb{R}^N$ the same as in Proposition 5, let $\boldsymbol{G} \in \mathbb{R}^{n \times N}$ and $\mathcal{N} := \mathcal{N}(\boldsymbol{A}) \cap \mathcal{N}(\boldsymbol{G})$. Then $\boldsymbol{G}\mathcal{M} \ominus \boldsymbol{G}\mathcal{S} = \boldsymbol{G}(\mathcal{M} \oplus \mathcal{N} \ominus \mathcal{S})$.

Proof: By Lemma 2, bullets i) and ii)

$$\begin{aligned} \boldsymbol{G}(\mathcal{M} \oplus \mathcal{N} \ominus \mathcal{S}) &\subseteq \boldsymbol{G}(\mathcal{M} \oplus \mathcal{N}) \ominus \boldsymbol{G}\mathcal{S} \\ &= \boldsymbol{G}\mathcal{M} \ominus \boldsymbol{G}\mathcal{S}. \end{aligned} \tag{19}$$

It remains to prove that $\boldsymbol{G}\mathcal{M} \ominus \boldsymbol{G}\mathcal{S} \subseteq \boldsymbol{G}(\mathcal{M} \oplus \mathcal{N} \ominus \mathcal{S})$. To this end, let $\boldsymbol{x} \in \boldsymbol{G}\mathcal{M} \ominus \boldsymbol{G}\mathcal{S}$ be arbitrary. Since $\boldsymbol{x} \oplus \boldsymbol{G}\mathcal{S} \subseteq \boldsymbol{G}\mathcal{M}$, we have

$$\forall \boldsymbol{\sigma} \in \mathcal{S} : \exists \boldsymbol{\mu}_{\boldsymbol{\sigma}} \in \mathcal{M} : \boldsymbol{x} + \boldsymbol{G}\boldsymbol{\sigma} = \boldsymbol{G}\boldsymbol{\mu}_{\boldsymbol{\sigma}}. \tag{20}$$

Now let $\boldsymbol{\sigma}, \boldsymbol{\sigma}' \in \mathcal{S}$ be arbitrary, Eq. (20) tells us

$$\boldsymbol{A}\boldsymbol{\mu}_{\boldsymbol{\sigma}} = \boldsymbol{A}\boldsymbol{\mu}_{\boldsymbol{\sigma}'} = \boldsymbol{b}, \tag{21}$$

$$\boldsymbol{G}(\underbrace{\boldsymbol{\mu}_{\boldsymbol{\sigma}} - \boldsymbol{\sigma}}_{=:\boldsymbol{\delta}_{\boldsymbol{\sigma}}}) = \boldsymbol{G}(\underbrace{\boldsymbol{\mu}_{\boldsymbol{\sigma}'} - \boldsymbol{\sigma}'}_{=:\boldsymbol{\delta}_{\boldsymbol{\sigma}'}}) = \boldsymbol{x}. \tag{22}$$

Clearly, $\boldsymbol{\delta}_{\boldsymbol{\sigma}} - \boldsymbol{\delta}_{\boldsymbol{\sigma}'} \in \mathcal{N}$ by Eqs. (21), (22) and the fact that $\boldsymbol{\sigma}, \boldsymbol{\sigma}' \in \mathcal{N}(\boldsymbol{A})$. This further implies that

$$\begin{aligned} \boldsymbol{\delta}_{\boldsymbol{\sigma}} + \boldsymbol{\sigma}' &= \boldsymbol{\delta}_{\boldsymbol{\sigma}'} - \boldsymbol{\delta}_{\boldsymbol{\sigma}'} + \boldsymbol{\delta}_{\boldsymbol{\sigma}} + \boldsymbol{\sigma}' \\ &= \boldsymbol{\mu}_{\boldsymbol{\sigma}'} + \underbrace{(\boldsymbol{\delta}_{\boldsymbol{\sigma}} - \boldsymbol{\delta}_{\boldsymbol{\sigma}'})}_{\in \mathcal{N}} \in \mathcal{M} \oplus \mathcal{N}. \end{aligned} \tag{23}$$

Since $\boldsymbol{\sigma}' \in \mathcal{S}$ is arbitrary, Eq. (23) implies that

$$\boldsymbol{\delta}_{\boldsymbol{\sigma}} \oplus \mathcal{S} \subseteq \mathcal{M} \oplus \mathcal{N} \iff \boldsymbol{\delta}_{\boldsymbol{\sigma}} \in \mathcal{M} \oplus \mathcal{N} \ominus \mathcal{S}. \tag{24}$$

Note that, by Eq. (20), $\boldsymbol{x} = \boldsymbol{G}(\boldsymbol{\mu}_{\boldsymbol{\sigma}} - \boldsymbol{\sigma}) = \boldsymbol{G}\boldsymbol{\delta}_{\boldsymbol{\sigma}}$. Combining this with Eq. (24) yields $\boldsymbol{x} \in \boldsymbol{G}(\mathcal{M} \oplus \mathcal{N} \ominus \mathcal{S})$. ■

Now we state the main result of this part.

Theorem 2. Let $\mathcal{CZ} = \langle \boldsymbol{G}, \boldsymbol{c}, \boldsymbol{A}, \boldsymbol{b} \rangle$ and $\mathcal{CZ}_\mathrm{s} = \langle \boldsymbol{G}\mathrm{diag}(\overline{\boldsymbol{\sigma}}), \boldsymbol{c}', \boldsymbol{A}\mathrm{diag}(\overline{\boldsymbol{\sigma}}), \mathbf{0} \rangle$, then $\mathcal{CZ}_\mathrm{d} = \langle \boldsymbol{G}\,\mathrm{diag}(\mathbf{1} - \overline{\boldsymbol{\sigma}}), \boldsymbol{c} - \boldsymbol{c}', \boldsymbol{A}\,\mathrm{diag}(\mathbf{1} - \overline{\boldsymbol{\sigma}}), \boldsymbol{b} \rangle \subseteq \mathcal{CZ} \ominus \mathcal{CZ}_\mathrm{s}$. Further, if $\mathcal{N} := \mathcal{N}(\boldsymbol{G}) \cap \mathcal{N}(\boldsymbol{A}) = \{\mathbf{0}\}$, we have $\mathcal{CZ}_\mathrm{d} = \mathcal{CZ} \ominus \mathcal{CZ}_\mathrm{s}$.

Proof: Note that $\mathcal{CZ}_\mathrm{s} = \boldsymbol{c}' + \boldsymbol{G}\mathcal{S}$ where $\mathcal{S} = \{\boldsymbol{\sigma} \in [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!] \mid \boldsymbol{A}\boldsymbol{\sigma} = \mathbf{0}\}$ (see Remark 2). Also note that $\mathcal{CZ} = \boldsymbol{c} + \boldsymbol{G}\mathcal{M}$ where $\mathcal{M} = \{\boldsymbol{\mu} \in [\![-\mathbf{1}, \mathbf{1}]\!] \mid \boldsymbol{A}\boldsymbol{\mu} = \boldsymbol{b}\} = \{\boldsymbol{\mu} \in [\![-\mathbf{1} + \overline{\boldsymbol{\sigma}}, \mathbf{1} - \overline{\boldsymbol{\sigma}}]\!] \oplus [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!] \mid \boldsymbol{A}\boldsymbol{\mu} = \boldsymbol{b}\}$. Define $\mathcal{D} = \{\boldsymbol{\delta} \in [\![-\mathbf{1} + \overline{\boldsymbol{\sigma}}, \mathbf{1} - \overline{\boldsymbol{\sigma}}]\!] \mid \boldsymbol{A}\boldsymbol{\delta} = \boldsymbol{b}\}$. We have $\mathcal{D} = \mathcal{M} \ominus \mathcal{S}$ by Remark 2 and Proposition 5. Also note that

$$\begin{aligned} &\mathcal{CZ} \ominus \mathcal{CZ}_\mathrm{s} \\ &= (\boldsymbol{c} - \boldsymbol{c}') + \boldsymbol{G}\mathcal{M} \ominus \boldsymbol{G}\mathcal{S} \\ &= (\boldsymbol{c} - \boldsymbol{c}') + \boldsymbol{G}(\mathcal{M} \oplus \mathcal{N} \ominus \mathcal{S}) && \text{(Proposition 6)} \\ &\supseteq (\boldsymbol{c} - \boldsymbol{c}') + \boldsymbol{G}(\mathcal{M} \ominus \mathcal{S} \oplus \mathcal{N}) && \text{(Lemma 2)} \\ &= (\boldsymbol{c} - \boldsymbol{c}') + \boldsymbol{G}(\mathcal{M} \ominus \mathcal{S}) \oplus \boldsymbol{G}\mathcal{N} && \text{(Lemma 2)} \\ &= (\boldsymbol{c} - \boldsymbol{c}') + \boldsymbol{G}(\mathcal{M} \ominus \mathcal{S}) && (\mathcal{N} \subseteq \mathcal{N}(G)) \\ &= (\boldsymbol{c} - \boldsymbol{c}') + \boldsymbol{G}\mathcal{D} = \mathcal{CZ}_\mathrm{d}. && \text{(Proposition 5)} \end{aligned} \tag{25}$$

Note that "$\supseteq$" in Eq. (25) holds as "$=$" if $\mathcal{N} = \{\mathbf{0}\}$. ■

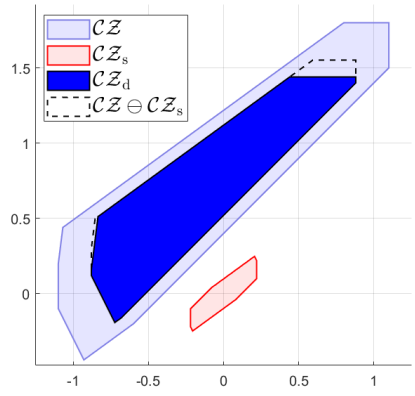

Fig. 1. Example 1.

Example 1. With an example, we illustrate that $\mathcal{CZ} \ominus \mathcal{CZ}_\mathrm{s} \neq \mathcal{CZ}_\mathrm{d}$ in general. Define

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 0 & 0.1 \\ 0 & 1 & 0 & 0.8 \end{bmatrix}, \qquad \boldsymbol{c} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \tag{26}$$

$$\boldsymbol{A} = \begin{bmatrix} -1 & 1 & 0.3 & 1 \end{bmatrix}, \qquad \boldsymbol{b} = 1, \tag{27}$$

and $\overline{\boldsymbol{\sigma}} = [0.2, 0.2, 0.2, 0.2]^\top$. Let $\mathcal{CZ} = \langle \boldsymbol{G}, \boldsymbol{c}, \boldsymbol{A}, \boldsymbol{b} \rangle$ and $\mathcal{CZ}_{\rm s}$ be defined as in Proposition 3. Fig. 1 shows that there is a gap between $\mathcal{CZ} \ominus \mathcal{CZ}_{\rm s}$ and its under-approximation $\mathcal{CZ}_{\rm d}$.

Remark 4. Since $\mathcal{CZ} \ominus \mathcal{CZ}_{\rm s} \supsetneq \mathcal{CZ}_{\rm d}$ in general, it is possible that $\mathcal{CZ} \ominus \mathcal{CZ}_{\rm s} \neq \emptyset$ but $\mathcal{CZ}_{\rm d} = \emptyset$. This issue can be mitigated by enforcing the following constraint in (min-out): $\boldsymbol{\theta} \in [\![-\mathbf{1} + \overline{\boldsymbol{\sigma}}, \mathbf{1} - \overline{\boldsymbol{\sigma}}]\!]$, $\boldsymbol{A}\boldsymbol{\theta} = \boldsymbol{b}$, where $\boldsymbol{\theta}$ is a decision variable. This extra constraint will ensure that $\mathcal{CZ}_{\rm d} \neq \emptyset$ whenever possible.

V. Exactness under a Rich CG-Rep of $\mathcal{CZ}$

The CG-Rep of a constrained zonotope is not unique. A notable feature of our two-step approach is: the obtained under-approximated difference $\mathcal{CZ}_{\rm d}$ varies with the CG-Rep of the minuend $\mathcal{CZ}$. In fact, if the CG-Rep of $\mathcal{CZ}$ is "rich" enough, the two-step approach is exact when $\mathcal{CZ} \ominus \mathcal{Z} \neq \emptyset$. Such a rich CG-Rep of $\mathcal{CZ}$ can be constructed as follows. Let

1) $\boldsymbol{H} \in \mathbb{R}^{\ell \times n}$, $\boldsymbol{a} \in \mathbb{R}^\ell$ be s.t. $\{\boldsymbol{x} \in \mathbb{R}^n \mid \boldsymbol{H}\boldsymbol{x} \leq \boldsymbol{a}\} = \mathcal{CZ}$;
2) $\boldsymbol{h}_i^\top \neq \mathbf{0}$ be the $i^{\rm th}$ row of $\boldsymbol{H}$ and a_i the $i^{\rm th}$ element of $\boldsymbol{a}$ (if $\boldsymbol{h}_i^\top = \mathbf{0}$, then $a_i = 0$ and this row can be removed);
3) $r > 0$ be a sufficiently large real number s.t. $\mathcal{CZ}_0 := \langle r\,\boldsymbol{I}_n, \boldsymbol{c} \rangle$ encloses $\mathcal{CZ}$ for some $\boldsymbol{c} \in \boldsymbol{c}' + (\mathcal{CZ} \ominus \mathcal{Z}) \neq \emptyset$, where $\boldsymbol{c}'$ is the center of $\mathcal{Z}$;
4) $\langle \boldsymbol{G}, \boldsymbol{c}, \boldsymbol{A}, \boldsymbol{b} \rangle$ be the CG-Rep of $\mathcal{CZ}_\ell$ obtained via iteratively applying Lemma 1 iv) to the following intersection operation, which leaves the center c unchanged:

$$\mathcal{CZ}_i = \mathcal{CZ}_{i-1} \cap \{\boldsymbol{x} \mid \boldsymbol{h}_i^\top \boldsymbol{x} \leq a_i\}, \quad i = 1, 2, \ldots, \ell. \tag{28}$$

Clearly, $\langle \boldsymbol{G}, \boldsymbol{c}, \boldsymbol{A}, \boldsymbol{b} \rangle$ is a CG-Rep of set $\mathcal{CZ}$ because $\langle \boldsymbol{G}, \boldsymbol{c}, \boldsymbol{A}, \boldsymbol{b} \rangle = \mathcal{CZ}_\ell = \{\boldsymbol{x} \mid \boldsymbol{H}\boldsymbol{x} \leq \boldsymbol{a}\} = \mathcal{CZ}$. To be precise,

$$\boldsymbol{G} = [r\,\boldsymbol{I}_n, \mathbf{0}_{n \times \ell}], \tag{29}$$
$$\boldsymbol{A} = [r\,\boldsymbol{H}, \operatorname{diag}(\tfrac{1}{2}\boldsymbol{d})], \tag{30}$$
$$d_i = a_i - \boldsymbol{h}_i^\top \boldsymbol{c} + r\|\boldsymbol{h}_i^\top\|_1, \ i = 1, 2, \ldots, \ell, \tag{31}$$
$$b_i = \tfrac{a_i - \boldsymbol{h}_i^\top \boldsymbol{c} - r\|\boldsymbol{h}_i^\top\|_1}{2}, \ i = 1, 2, \ldots, \ell, \tag{32}$$

where d_i (b_i, resp.) is the $i^{\rm th}$ element of vector $\boldsymbol{d}$ ($\boldsymbol{b}$, resp.).

In the rest of this section, we use $\langle \boldsymbol{G}, \boldsymbol{c}, \boldsymbol{A}, \boldsymbol{b} \rangle$ as the CG-Rep of the minuend $\mathcal{CZ}$ and show that Step I and Step II are exact when $\mathcal{CZ} \ominus \mathcal{Z} \neq \emptyset$.

The following lemma will be useful.

Lemma 5. Assume that $\mathcal{CZ} \ominus \mathcal{Z} \neq \emptyset$, then $d_i > 0$ and $[\boldsymbol{G}; \boldsymbol{A}]$ is invertible.

Proof: Recall that $\mathcal{CZ} = \{\boldsymbol{x} \mid \boldsymbol{H}\boldsymbol{x} \leq \boldsymbol{a}\}$, $\mathcal{Z} = \langle \boldsymbol{c}', \boldsymbol{G}' \rangle$. Since $\boldsymbol{c} \in \boldsymbol{c}' + (\mathcal{CZ} \ominus \mathcal{Z})$, i.e., $\boldsymbol{c} - \boldsymbol{c}' + \mathcal{Z} \subseteq \mathcal{CZ}$, we have

$$a_i \geq \max \boldsymbol{h}_i^\top (\boldsymbol{c} - \boldsymbol{c}' + \mathcal{Z}) = \boldsymbol{h}_i^\top \boldsymbol{c} + \|\boldsymbol{h}_i^\top \boldsymbol{G}'\|_1. \tag{33}$$

By Eqs. (31), (33), $d_i \geq \|\boldsymbol{h}_i^\top \boldsymbol{G}'\|_1 + r\|\boldsymbol{h}_i^\top\|_1$. Since $\boldsymbol{h}_i \neq \mathbf{0}$ and $r > 0$ (see bullets 2), 3)), $d_i > 0$.

By Eqs. (29), (30), $[\boldsymbol{G}; \boldsymbol{A}] = [r\,\boldsymbol{I}_n, \mathbf{0}; r\,\boldsymbol{H}, \operatorname{diag}(\frac{\boldsymbol{d}}{2})] \in \mathbb{R}^{(n+\ell)\times(n+\ell)}$. Since $r > 0$ and $d_i > 0$ for $i = 1, 2, \ldots, \ell$, $[\boldsymbol{G}; \boldsymbol{A}]$ is a triangular matrix with non-zero diagonal entries. Therefore $[\boldsymbol{G}; \boldsymbol{A}]$ is invertible. ∎

The following result says that Step I is exact.

Proposition 7. Suppose that $\mathcal{CZ} \ominus \mathcal{Z} \neq \emptyset$, then (simple) is feasible. Moreover, let $\boldsymbol{\Gamma}$ be the minimizer of (simple), define $\overline{\boldsymbol{\sigma}} = |\boldsymbol{\Gamma}|\mathbf{1}$ and $\mathcal{CZ}_{\rm s} = \langle \boldsymbol{G} \operatorname{diag}(\overline{\boldsymbol{\sigma}}), \boldsymbol{c}', \boldsymbol{A} \operatorname{diag}(\overline{\boldsymbol{\sigma}}), \mathbf{0} \rangle$, then $\mathcal{CZ} \ominus \mathcal{CZ}_{\rm s} = \mathcal{CZ} \ominus \mathcal{Z}$.

Proof: By Lemma 5, there is a unique $\boldsymbol{\Gamma}$ satisfying the equality constraint $[\boldsymbol{G}; \boldsymbol{A}]\boldsymbol{\Gamma} = [\boldsymbol{G}'; \mathbf{0}]$, i.e.,

$$\boldsymbol{\Gamma} = \big[\tfrac{1}{r}\boldsymbol{G}'; -\operatorname{diag}(\tfrac{\boldsymbol{d}}{2})^{-1}\boldsymbol{H}\boldsymbol{G}'\big], \tag{34}$$

In what follows, we show that, assuming that $\langle r\,\boldsymbol{I}_n, \boldsymbol{c} \rangle \supseteq \mathcal{CZ}$, the constraint $|\boldsymbol{\Gamma}|\mathbf{1} \leq \mathbf{1}$ holds automatically. Note that

$$\overline{\boldsymbol{\sigma}} = |\boldsymbol{\Gamma}|\mathbf{1} = \Big[\tfrac{1}{r}|\boldsymbol{G}'|\mathbf{1}; \big|\operatorname{diag}(\tfrac{\boldsymbol{d}}{2})^{-1}\boldsymbol{H}\boldsymbol{G}'\big|\mathbf{1}\Big]. \tag{35}$$

i) For $j = 1, 2 \ldots, n$, $\overline{\sigma}_j = \frac{1}{r}\|\boldsymbol{e}_j^\top \boldsymbol{G}'\|_1$ where $\boldsymbol{e}_j$ is the $j^{\rm th}$ natural basis. Since $\langle r\,\boldsymbol{I}_n, \boldsymbol{c} \rangle \supseteq \mathcal{CZ} \supseteq \boldsymbol{c} - \boldsymbol{c}' + \mathcal{Z} = \langle \boldsymbol{G}', \boldsymbol{c}' \rangle$, we have

$$\begin{aligned} &\boldsymbol{e}_j^\top \boldsymbol{c}' + \|\boldsymbol{e}_j^\top \boldsymbol{G}'\|_1 = \max \boldsymbol{e}_j^\top (\boldsymbol{c} - \boldsymbol{c}' + \mathcal{Z}) \\ &\leq \max \boldsymbol{e}_j^\top \langle r\,\boldsymbol{I}_n, \boldsymbol{c} \rangle = \boldsymbol{e}_j^\top \boldsymbol{c}' + r. \end{aligned} \tag{36}$$

Therefore $\|\boldsymbol{e}_j^\top \boldsymbol{G}'\|_1 \leq r$ and $\overline{\sigma}_j \leq 1$.

ii) For $i = 1, 2, \ldots, \ell$, $\overline{\sigma}_{n+i} = \frac{2}{d_i}\|\boldsymbol{h}_i^\top \boldsymbol{G}'\|_1 = \frac{2\|\boldsymbol{h}_i^\top \boldsymbol{G}'\|_1}{\|\boldsymbol{h}_i^\top \boldsymbol{G}'\|_1 + r\|\boldsymbol{h}_i^\top\|_1}$. Again, since $\langle r\,\boldsymbol{I}_n, \boldsymbol{c} \rangle \supseteq \boldsymbol{c} - \boldsymbol{c}' + \mathcal{Z} = \langle \boldsymbol{G}', \boldsymbol{c}' \rangle$, we have

$$\begin{aligned} &\boldsymbol{h}_i^\top \boldsymbol{c} + \|\boldsymbol{h}_i^\top \boldsymbol{G}'\|_1 = \max \boldsymbol{h}_i^\top (\boldsymbol{c} - \boldsymbol{c}' + \mathcal{Z}) \\ &\leq \max \boldsymbol{h}_i^\top \langle r\,\boldsymbol{I}_n, \boldsymbol{c} \rangle = \boldsymbol{h}_i^\top \boldsymbol{c} + r\|\boldsymbol{h}_i^\top\|_1. \end{aligned} \tag{37}$$

Therefore $\|\boldsymbol{h}_i^\top \boldsymbol{G}'\|_1 \leq r\|\boldsymbol{h}_i^\top\|_1$ and $\overline{\sigma}_{n+i} \leq 1$.

So far we have proved that $\boldsymbol{\Gamma}$ is the unique feasible solution (hence the minimizer) of (simple).

It is known from Lemma 4 that $\mathcal{CZ} \ominus \mathcal{Z} = \mathcal{CZ} \ominus \{\boldsymbol{x} \mid \boldsymbol{H}\boldsymbol{x} \leq \boldsymbol{a}_{\rm s}\}$, where $\boldsymbol{a}_{\rm s} \in \mathbb{R}^\ell$ and its $i^{\rm th}$ element $a_{{\rm s},i} = \boldsymbol{h}_i^\top \boldsymbol{c}' + \|\boldsymbol{h}_i^\top \boldsymbol{G}'\|_1$. Note that, for $i = 1, 2, \ldots, \ell$,

$$\begin{aligned} &\max \boldsymbol{h}_i^\top \mathcal{CZ}_{\rm s} \\ &= \max \boldsymbol{h}_i^\top \{\boldsymbol{G}\boldsymbol{\sigma} + \boldsymbol{c}' \mid \boldsymbol{\sigma} \in [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!], \boldsymbol{A}\boldsymbol{\sigma} = \mathbf{0}\} \\ &= \boldsymbol{h}_i^\top \boldsymbol{c}' + \max \left\{ r\,\boldsymbol{h}_i^\top \boldsymbol{\sigma}_{1:n} \,\middle|\, \begin{array}{l} \boldsymbol{\sigma} \in [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!], \ r\boldsymbol{H}\boldsymbol{\sigma}_{1:n} = \\ -\operatorname{diag}(\frac{\boldsymbol{d}}{2})\boldsymbol{\sigma}_{n+1:n+\ell} \end{array} \right\} \\ &\leq \boldsymbol{h}_i^\top \boldsymbol{c}' + \max\{-\tfrac{d_i}{2}\sigma_{n+i} \mid \boldsymbol{\sigma} \in [\![-\overline{\boldsymbol{\sigma}}, \overline{\boldsymbol{\sigma}}]\!]\} \\ &= \boldsymbol{h}_i^\top \boldsymbol{c}' + \tfrac{d_i}{2}\overline{\sigma}_{n+i} \\ &= \boldsymbol{h}_i^\top \boldsymbol{c}' + \|\boldsymbol{h}_i^\top \boldsymbol{G}'\|_1 = a_{{\rm s},i}, \end{aligned} \tag{38}$$

where $\boldsymbol{\sigma}_{1:n}$ (and $\boldsymbol{\sigma}_{n+1:n+\ell}$, resp.) is a vector that consists of the first n elements (and the last ℓ elements, resp.) of $\boldsymbol{\sigma}$. By Eq. (38), $\mathcal{CZ}_{\rm s} \subseteq \{\boldsymbol{x} \mid \boldsymbol{H}\boldsymbol{x} \leq \boldsymbol{a}_{\rm s}\}$. Together with the fact that $\mathcal{Z} \subseteq \mathcal{CZ}_{\rm s}$, we have $\mathcal{CZ} \ominus \mathcal{CZ}_{\rm s} = \mathcal{CZ} \ominus \mathcal{Z}$. ∎

The following result says that Step II is exact.

Proposition 8. Let $\mathcal{CZ}_{\rm s} = \langle \boldsymbol{G} \operatorname{diag}(\overline{\boldsymbol{\sigma}}), \boldsymbol{c}', \boldsymbol{A} \operatorname{diag}(\overline{\boldsymbol{\sigma}}), \mathbf{0} \rangle$ and $\mathcal{CZ}_{\rm d} = \langle \boldsymbol{G} \operatorname{diag}(\mathbf{1} - \overline{\boldsymbol{\sigma}}), \boldsymbol{c} - \boldsymbol{c}', \boldsymbol{A} \operatorname{diag}(\mathbf{1} - \overline{\boldsymbol{\sigma}}), \boldsymbol{b} \rangle$, where $\overline{\boldsymbol{\sigma}}$ is defined the same as in Proposition 7, then $\mathcal{CZ} \ominus \mathcal{CZ}_{\rm s} = \mathcal{CZ}_{\rm d}$.

Proof: By Lemma 5, $\mathcal{N}(\boldsymbol{G}) \cap \mathcal{N}(\boldsymbol{A}) = \mathcal{N}([\boldsymbol{G}; \boldsymbol{A}]) = \{\mathbf{0}\}$. By Theorem 2, $\mathcal{CZ} \ominus \mathcal{CZ}_{\rm s} = \mathcal{CZ}_{\rm d}$. ∎

Although $\mathcal{CZ} \ominus \mathcal{Z} \neq \emptyset$ is assumed in Propositions 7, 8, the result $\mathcal{CZ}_{\rm d}$ returned by the two-step approach is exact in the following sense, regardless of this assumption.

Theorem 3. For any constrained zonotope $\mathcal{CZ}$, if we construct its CG-Rep following steps 1)-4), then the followings hold:

i) if $\mathcal{CZ} \ominus \mathcal{Z} = \emptyset$, either $\mathcal{CZ}_{\rm d} = \emptyset$ or (simple) is infeasible;
ii) if $\mathcal{CZ} \ominus \mathcal{Z} \neq \emptyset$, $\mathcal{CZ}_{\rm d} = \mathcal{CZ} \ominus \mathcal{Z}$.

Proof: Bullet ii) follows from Proposition 7 and Proposition 8. For bullet i), if (simple) is feasible, then $\mathcal{CZ}_{\rm d} = \emptyset$ because $\mathcal{CZ}_{\rm d} \subseteq \mathcal{CZ} \ominus \mathcal{Z} = \emptyset$ by Theorem 2. ■

Remark 5. The run time of our two-step approach is polynomial in the input size. By Example 1, this approach is not exact *in general*. However, as stated by Theorem 3, the two-step approach still achieves exactness *in special cases* where $\mathcal{CZ}$'s CG-Rep is not the most "compact" one. Note that, such non-compact CG-Rep is constructed from the H-Rep of $\mathcal{CZ}$, whose complexity may, in the worst case, be exponential in that of $\mathcal{CZ}$'s most compact CG-Rep. Therefore, the exactness results are not surprising because in this case, the two-step approach bypasses the high-complexity step of computing $\mathcal{CZ}$'s H-Rep. This is also consistent with the fact that Minkowski-subtracting a zonotope from a polytope in its H-Rep is easy [14]. However, our results in Sec. V may open the direction of incrementally enriching the minuend's CG-Rep to achieve exact results quickly whenever possible.

VI. Backward Reachable Set Computation for Nonlinear Systems

In this section, we use our two-step approach from Sec. IV to develop BRS under-approximation algorithms for system (2). To incorporate the error introduced by sequential linearization, we require $\underline{\mathcal{X}}_{k-1} \ominus \mathcal{L}$ to be reachable from $\underline{\mathcal{X}}_k$ under the linearized dynamics, where $\underline{\mathcal{X}}_{k-1}$ ($\underline{\mathcal{X}}_k$, resp.) are the $k-1^{\rm st}$ ($k^{\rm th}$, resp.) under-approximated BRS and $\mathcal{L}$ contains all values of the linearization error over $\underline{\mathcal{X}}_k$. As mentioned in Sec. III, the challenge is to approximate $\mathcal{L}$ without knowing $\underline{\mathcal{X}}_k$ a priori. To resolve this issue, we explore the following two strategies.

A) Scaling method: we incrementally enlarge $\mathcal{L}$ by a scaling factor until i) $\underline{\mathcal{X}}_{k-1} \ominus \mathcal{L}$ is reachable from $\underline{\mathcal{X}}_k$ under the linear dynamics, and ii) $\mathcal{L}$ encompasses all the values of the linearization error in $\underline{\mathcal{X}}_k$. Here, each $\underline{\mathcal{X}}_k$ is a constrained zonotope.
B) Splitting method: we fix $\mathcal{L}$ and split $\underline{\mathcal{X}}_{k-1}$ into finitely many smaller sets, i.e., $\underline{\mathcal{X}}_{k-1} = \bigcup_i \underline{\mathcal{X}}^i_{k-1}$. The nonlinear system is linearized for each $\underline{\mathcal{X}}^i_{k-1}$, and the splitting procedure terminates when the linearization error in each $\underline{\mathcal{X}}^i_k$, from where $\underline{\mathcal{X}}^i_{k-1} \ominus \mathcal{L}$ is reachable under the $i^{\rm th}$ linear dynamics, are contained by $\mathcal{L}$. In this case, $\underline{\mathcal{X}}_k = \bigcup_i \underline{\mathcal{X}}^i_k$ and is represented by the collection of the CG-Reps of constrained zonotopic sets $\underline{\mathcal{X}}^i_k$.

The scaling method is in principle similar to the approach proposed in [24], and the splitting method borrows the idea from [25], where a similar splitting procedure is developed for zonotopes to control the linearization error in forward reachability analysis. Unique to our implementation is the use of our efficient Minkowski-difference computation techniques tailored to constrained zonotopes. While the scaling method better suits the computation with more steps (i.e., larger k) in a convex safe set $\mathcal{X}_{\rm safe}$, the splitting method better captures the shape of a nonconvex set $\mathcal{X}_k$ and is more suitable when $\mathcal{X}_{\rm safe}$ is also nonconvex, because $\underline{\mathcal{X}}_k$ is represented as a collection of constrained zonotopes in the latter method. In what follows, we present the detailed algorithms for the two methods above.

A. Scaling Method

Algorithm 1 $\underline{\mathcal{X}}_k = \text{ScalingBRS}(\underline{\mathcal{X}}_{k-1}, \boldsymbol{f}, \mathcal{U}, \mathcal{W}, \mathcal{X}_{\rm safe})$

Input: Constrained zonotope $\underline{\mathcal{X}}_{k-1}$; System's vector field $\boldsymbol{f}$; Control input set $\mathcal{U}$; Disturbance set $\mathcal{W}$; Safe set $\mathcal{X}_{\rm safe}$
Output: Constrained zonotope $\underline{\mathcal{X}}_k \subseteq Pre(\underline{\mathcal{X}}_{k-1})$

1: $\widetilde{\boldsymbol{z}} \leftarrow center(\underline{\mathcal{X}}_{k-1} \times \mathcal{U})$
2: $[\widetilde{\boldsymbol{A}}, \widetilde{\boldsymbol{B}}] \leftarrow linearize(\widetilde{\boldsymbol{z}}, \boldsymbol{f})$; $\widetilde{\mathcal{L}} \leftarrow \{\boldsymbol{f}(\widetilde{\boldsymbol{z}}) - [\widetilde{\boldsymbol{A}}, \widetilde{\boldsymbol{B}}]\widetilde{\boldsymbol{z}}\}$
3: $\widetilde{\mathcal{Z}}_k \leftarrow Pre_{\boldsymbol{x},\boldsymbol{u}}(\underline{\mathcal{X}}_{k-1}, \widetilde{\boldsymbol{A}}, \widetilde{\boldsymbol{B}}, \mathcal{U}, \mathcal{W}, \widetilde{\mathcal{L}}, \mathcal{X}_{\rm safe})$
4: $\boldsymbol{z}^* \leftarrow center(\widetilde{\mathcal{Z}}_k)$
5: $[\boldsymbol{A}, \boldsymbol{B}] \leftarrow linearize(\boldsymbol{z}^*, \boldsymbol{f})$; $\mathcal{L} \leftarrow LE(\boldsymbol{z}^*, \boldsymbol{f}, \widetilde{\mathcal{Z}}_k)$
6: $\mathcal{Z}_k \leftarrow Pre_{\boldsymbol{x},\boldsymbol{u}}(\underline{\mathcal{X}}_{k-1}, \boldsymbol{A}, \boldsymbol{B}, \mathcal{U}, \mathcal{W}, \mathcal{L}, \mathcal{X}_{\rm safe})$
7: **while** $LE(\boldsymbol{z}^*, \boldsymbol{f}, \mathcal{Z}_k) \not\subseteq \mathcal{L}$ **do**
8: Enlarge $\mathcal{L}$ by a factor α
9: $\mathcal{Z}_k \leftarrow Pre_{\boldsymbol{x},\boldsymbol{u}}(\underline{\mathcal{X}}_{k-1}, \boldsymbol{A}, \boldsymbol{B}, \mathcal{U}, \mathcal{W}, \mathcal{L}, \mathcal{X}_{\rm safe})$
10: **return** $\underline{\mathcal{X}}_k \leftarrow Proj_{\boldsymbol{x}}(\mathcal{Z}_k)$

Algorithm 1 details the scaling method. In this algorithm, we first linearize the system at the geometric center $\widetilde{z}$ of the interval closure of $\underline{\mathcal{X}}_{k-1} \times \mathcal{U}$. The function $center(\mathcal{Z})$ returns $\frac{1}{2}(\underline{\boldsymbol{z}} + \overline{\boldsymbol{z}})$, where $\underline{\boldsymbol{z}}$ and $\overline{\boldsymbol{z}}$ are the lower and upper limits of the smallest hyper-box that contains set $\mathcal{Z}$. That is,

$$\underline{z}_i = \min \boldsymbol{e}_i^\top \mathcal{Z}, \qquad \overline{z}_i = \max \boldsymbol{e}_i^\top \mathcal{Z}, \tag{39}$$

where $\underline{z}_i$ and $\overline{z}_i$ are the $i^{\rm th}$ elements of $\underline{\boldsymbol{z}}$ and $\overline{\boldsymbol{z}}$, respectively. Suppose that $\mathcal{Z}$ is a constrained zonotope, executing the function $center$ amounts to solving $2n$ linear programs. On line 2, the function $linearize(\boldsymbol{z}, \boldsymbol{f})$ linearizes the vector field $\boldsymbol{f}$ at point $\boldsymbol{z}$ and returns the matrices that define the obtained linear system, i.e.,

$$\boldsymbol{A} = \left.\frac{\partial \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{u})}{\partial \boldsymbol{x}}\right|_{[\boldsymbol{x};\boldsymbol{u}]=\boldsymbol{z}}, \quad \boldsymbol{B} = \left.\frac{\partial \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{u})}{\partial \boldsymbol{u}}\right|_{[\boldsymbol{x};\boldsymbol{u}]=\boldsymbol{z}}. \tag{40}$$

On line 3, we compute a set $\widetilde{\mathcal{Z}}_k$ of state-input vectors $[\boldsymbol{x}; \boldsymbol{u}]$ such that $\underline{\mathcal{X}}_{k-1}$ is reached from state $\boldsymbol{x}$ under control $\boldsymbol{u}$ and the obtained linear dynamics. To be precise, $Pre_{\boldsymbol{x},\boldsymbol{u}}(\mathcal{X}, \boldsymbol{A}, \boldsymbol{B}, \mathcal{U}, \mathcal{W}, \mathcal{L}, \mathcal{X}_{\rm safe})$ is defined to be:

$$\{[\boldsymbol{x}; \boldsymbol{u}] \in \mathcal{X}_{\rm safe} \times \mathcal{U} \mid \boldsymbol{A}\boldsymbol{x} + \boldsymbol{B}\boldsymbol{u} \in \mathcal{X} \ominus (\mathcal{L} \oplus \mathcal{W})\}. \tag{41}$$

Suppose that $\mathcal{X}_{\rm safe}$ is a polytope, then $Pre_{\boldsymbol{x},\boldsymbol{u}}$ is a constrained zonotope whose CG-Rep can be obtained using Lemma 1 and our two-step approach for Minkowski-difference computation. Note that, in line 3, $\widetilde{\mathcal{Z}}_k$ is computed without considering any linearization error (i.e., $\widetilde{\mathcal{L}} = \{\boldsymbol{f}(\widetilde{\boldsymbol{z}}) - [\widetilde{\boldsymbol{A}}, \widetilde{\boldsymbol{B}}]\widetilde{\boldsymbol{z}}\}$ is a singleton set). The purpose of this step is to find a better point

$\boldsymbol{z}^* = center(\widetilde{\mathcal{Z}}_k)$ to linearize the system at (line 4). Then on lines 5-6, we linearize the system at $\boldsymbol{z}^*$ and recompute a set $\mathcal{Z}_k$ with the latest linear system and a set $\mathcal{L} = LE(\boldsymbol{z}^*, \boldsymbol{f}, \widetilde{\mathcal{Z}}_k)$ that contains all possible values of the linearization error. Particularly, $LE(\boldsymbol{z}^*, \boldsymbol{f}, \mathcal{Z})$ is a zonotope that encloses the following set of Lagrange remainders over set $\mathcal{Z}$:

$$\boldsymbol{f}(\boldsymbol{z}^*) - [\boldsymbol{A}, \boldsymbol{B}]\boldsymbol{z}^* + \left\{ \boldsymbol{L} \in \mathbb{R}^n \,\middle|\, \begin{matrix} L_i = \frac{1}{2}(\boldsymbol{z} - \boldsymbol{z}^*)^\top \frac{\partial^2 f_i}{\partial \boldsymbol{z}^2}(\boldsymbol{\xi}_i)(\boldsymbol{z} - \boldsymbol{z}^*), \ \boldsymbol{z} \in \mathcal{Z} \\ \boldsymbol{\xi}_i = \lambda_i \boldsymbol{z}^* + (1 - \lambda_i)\boldsymbol{z}, \ \lambda_i \in [\![0, 1]\!] \end{matrix} \right\} \quad (42)$$

where $\boldsymbol{A}$, $\boldsymbol{B}$ are given by Eq. (40) evaluated at $\boldsymbol{z}^*$, and L_i, f_i are the i^{th} elements of $\boldsymbol{L}$ and $\boldsymbol{f}$, respectively. The set $LE(\boldsymbol{z}^*, \boldsymbol{f}, \mathcal{Z})$ can be computed as a hyper-box using interval analysis techniques (e.g., see [25]). If $\mathcal{L}$ encloses all possible values of the linearization error in set $\mathcal{Z}_k$, then $\mathcal{X}_{k-1}$ can be reached from $Proj_{\boldsymbol{x}}(\mathcal{Z}_k) := \{\boldsymbol{x} \mid [\boldsymbol{x}; \boldsymbol{u}] \in \mathcal{Z}_k\}$ under the nonlinear dynamics[2]. In that case, we return $\underline{\mathcal{X}}_k = Proj_{\boldsymbol{x}}(\mathcal{Z}_k)$. Otherwise we incrementally enlarge $\mathcal{L}$ by a factor α and recompute $\mathcal{Z}_k$ until the linearization error set $LE(\boldsymbol{z}^*, \boldsymbol{f}, \mathcal{Z}_k)$ is enclosed by $\mathcal{L}$.

B. Splitting Method

The real backward reachable set $\mathcal{X}_k$ may not be convex due to the nonlinearity of the system's vector field $\boldsymbol{f}$ or the nonconvexity of the safe set $\mathcal{X}_{\text{safe}}$. Therefore, the scaling method can be conservative because we under-approximate a potentially nonconvex set $\mathcal{X}_k$ with a constrained zonotope $\underline{\mathcal{X}}_k$, which is a convex set. In this part, we present the splitting method, where the linearization error set $\mathcal{L}$ is defined to have a prescribed (i.e., fixed) size, and $\underline{\mathcal{X}}_k$ is represented as the *union* of a finite collection $\{\underline{\mathcal{X}}_k^i\}$ of constrained zonotopes, so that the linearization error in each $\underline{\mathcal{X}}_k^i$ is over-approximated by the prescribed $\mathcal{L}$. Since $\underline{\mathcal{X}}_k = \bigcup_i \underline{\mathcal{X}}_k^i$ is not necessarily convex in the splitting method, it serves as a less conservative (i.e., larger) under-approximation of $\mathcal{X}_k$.

The following proposition provides a rigorous way to split one constrained zonotope into two, so that the linearization error can be evaluated over the two smaller sets separately.

Proposition 9. Assume that $\mathcal{CZ} = \langle \boldsymbol{G}, \boldsymbol{c}, \boldsymbol{A}, \boldsymbol{b} \rangle$, where $\boldsymbol{G} = [\boldsymbol{g}_1, \boldsymbol{g}_2, \cdots, \boldsymbol{g}_N], \boldsymbol{A} = [\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_N]$. Then set $\mathcal{CZ}$ can be split into $\mathcal{CZ}_1^i = \langle \boldsymbol{G}_1, \boldsymbol{c}_1, \boldsymbol{A}_1, \boldsymbol{b}_1 \rangle$ and $\mathcal{CZ}_2^i = \langle \boldsymbol{G}_2, \boldsymbol{c}_2, \boldsymbol{A}_2, \boldsymbol{b}_2 \rangle$ along $\boldsymbol{g}_i$, i.e., $\mathcal{CZ} = \mathcal{CZ}_1^i \cup \mathcal{CZ}_2^i$ where

$$\boldsymbol{G}_1 = \boldsymbol{G}_2 = [\boldsymbol{g}_1, \boldsymbol{g}_2, \cdots, \tfrac{1}{2}\boldsymbol{g}_i, \cdots, \boldsymbol{g}_N] \quad (43)$$

$$\boldsymbol{A}_1 = \boldsymbol{A}_2 = [\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \tfrac{1}{2}\boldsymbol{a}_i, \cdots, \boldsymbol{a}_N] \quad (44)$$

$$\boldsymbol{b}_1 = \boldsymbol{b} - \tfrac{1}{2}\boldsymbol{a}_i \quad \boldsymbol{c}_1 = \boldsymbol{c} + \tfrac{1}{2}\boldsymbol{g}_i \quad (45)$$

$$\boldsymbol{b}_2 = \boldsymbol{b} + \tfrac{1}{2}\boldsymbol{a}_i \quad \boldsymbol{c}_2 = \boldsymbol{c} - \tfrac{1}{2}\boldsymbol{g}_i \quad (46)$$

Proof: The set $\mathcal{CZ}$ can be written as

$$\mathcal{CZ} = \{\boldsymbol{G}\boldsymbol{\theta} + \boldsymbol{c} \mid |\theta_j| \le 1, j = 1, 2, \cdots, N, \boldsymbol{A}\boldsymbol{\theta} = \boldsymbol{b}\}. \quad (47)$$

[2]The projection step amounts to a linear transformation and is easy for CG-Reps by Lemma 1, bullet i).

where $\boldsymbol{\theta} = [\theta_1; \theta_2; \cdots; \theta_N] \in \mathbb{R}^N$. Define

$$\mathcal{CZ}_1^i = \{\boldsymbol{G}\boldsymbol{\theta} + \boldsymbol{c} \,|\, \theta_i \in [\![0, 1]\!], |\theta_j| \le 1, j \ne i, \boldsymbol{A}\boldsymbol{\theta} = \boldsymbol{b}\}, \quad (48)$$

$$\mathcal{CZ}_2^i = \{\boldsymbol{G}\boldsymbol{\theta} + \boldsymbol{c} \,|\, \theta_i \in [\![-1, 0]\!], |\theta_j| \le 1, j \ne i, \boldsymbol{A}\boldsymbol{\theta} = \boldsymbol{b}\}. \quad (49)$$

Apparently, $\mathcal{CZ} = \mathcal{CZ}_1^i \cup \mathcal{CZ}_2^i$. To show that $\mathcal{CZ}_1^i = \langle \boldsymbol{G}_1, \boldsymbol{c}_1, \boldsymbol{A}_1, \boldsymbol{b}_1 \rangle$, let $\boldsymbol{\theta}$ be such that $\theta_i \in [\![0, 1]\!]$, $|\theta_j| \le 1$ for all $j \ne i$ and $\boldsymbol{A}\boldsymbol{\theta} = \boldsymbol{b}$. Define $\mu_i = 2\theta_i - 1$ and $\hat{\boldsymbol{\theta}} = [\theta_1, \theta_2, \cdots, \theta_{i-1}; \mu_i; \theta_{i+1}; \cdots; \theta_N]^\top$, then

$$\begin{aligned} \boldsymbol{G}\boldsymbol{\theta} + \boldsymbol{c} &= \boldsymbol{c} + \textstyle\sum_{j=1, j\ne i}^N \boldsymbol{g}_j\theta_j + \boldsymbol{g}_i(\tfrac{1}{2}\mu_i + \tfrac{1}{2}) \\ &= (\boldsymbol{c} + \tfrac{1}{2}\boldsymbol{g}_i) + \textstyle\sum_{j=1, j\ne i}^N \boldsymbol{g}_j\theta_j + \tfrac{1}{2}\boldsymbol{g}_i\mu_i \\ &= \boldsymbol{G}_1\hat{\boldsymbol{\theta}} + \boldsymbol{c}_1 \end{aligned} \quad (50)$$

In addition,

$$\begin{aligned} \boldsymbol{A}\boldsymbol{\theta} = \boldsymbol{b} &\iff \textstyle\sum_{j=1}^N \boldsymbol{a}_j\theta_j = \boldsymbol{b} \\ &\iff \textstyle\sum_{j=1, j\ne i}^N \boldsymbol{a}_j\theta_j + \boldsymbol{a}_i(\tfrac{1}{2}\mu_i + \tfrac{1}{2}) = \boldsymbol{b} \\ &\iff \boldsymbol{A}_1\hat{\boldsymbol{\theta}} = \boldsymbol{b}_1 \end{aligned} \quad (51)$$

Since $|\mu_i| = |2\theta_i - 1| \le 1$, we have $\hat{\boldsymbol{\theta}} \in [\![\boldsymbol{0}, \boldsymbol{1}]\!]$. Therefore,

$$\begin{aligned} \mathcal{CZ}_1^i &= \{\boldsymbol{G}_1\hat{\boldsymbol{\theta}} + \boldsymbol{c}_1 \mid \hat{\boldsymbol{\theta}} \in [\![\boldsymbol{0}, \boldsymbol{1}]\!], \boldsymbol{A}_1\hat{\boldsymbol{\theta}} = \boldsymbol{b}_1\} \\ &= \langle \boldsymbol{G}_1, \boldsymbol{c}_1, \boldsymbol{A}_1, \boldsymbol{b}_1 \rangle \end{aligned} \quad (52)$$

Similarly, to show that $\mathcal{CZ}_2^i = \langle \boldsymbol{G}_2, \boldsymbol{c}_2, \boldsymbol{A}_2, \boldsymbol{b}_2 \rangle$, let $\boldsymbol{\theta}$ be such that $\theta_i \in [\![-1, 0]\!]$, $|\theta_j| \le 1$ for all $j \ne i$ and $\boldsymbol{A}\boldsymbol{\theta} = \boldsymbol{b}$. The above argument follows by setting $\mu_i = 2\theta_i + 1$. ■

Fig. 2 shows the two sets $\mathcal{CZ}_1$ (green) and $\mathcal{CZ}_2$ (red) obtained by splitting $\mathcal{CZ}$ (black contour) using Proposition 9. Note that $\mathcal{CZ}_1$ overlaps with $\mathcal{CZ}_2$. As we will see, this overlap helps to reduce the conservatism in the BRS computation.

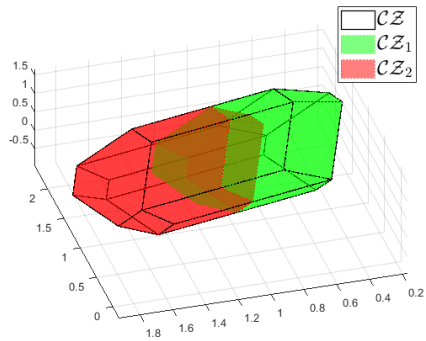

Fig. 2. Result for Proposition 9: $\mathcal{CZ} = \mathcal{CZ}_1 \cup \mathcal{CZ}_2$

Based on Proposition 9, a detailed algorithm that implements the splitting method is given in Algorithm 2. The input $\{\underline{\mathcal{X}}_k^\ell\}$ and the output $\{\underline{\mathcal{X}}_{k-1}^i\}$ are finite collections of constrained zonotopes s.t. $\underline{\mathcal{X}}_{k-1} = \bigcup_i \underline{\mathcal{X}}_{k-1}^i$ and $\underline{\mathcal{X}}_k = \bigcup_\ell \underline{\mathcal{X}}_k^\ell$ are the under-approximation of the $k-1^{\text{st}}$ and the k^{th} BRSs, respectively. The sub-procedures $center$, $linearize$ and LE are the same as in the scaling method. However, $Pre_{\boldsymbol{x},\boldsymbol{u}}(\mathcal{X}, \boldsymbol{A}, \boldsymbol{B}, \mathcal{U}, \mathcal{W}, \mathcal{L})$, which computes the extended constrained zonotope $\mathcal{Z}$, has a slightly different definition, i.e.,

$$\mathcal{Z} = \{[\boldsymbol{x}; \boldsymbol{u}] \mid \boldsymbol{A}\boldsymbol{x} + \boldsymbol{B}\boldsymbol{u} \in \mathcal{X} \ominus (\mathcal{L} \oplus \mathcal{W}), u \in \mathcal{U}\}. \quad (53)$$

In Eq. (53), $\boldsymbol{x} \in \mathcal{X}_{\text{safe}}$ is not enforced as in the scaling method.

Algorithm 2 is briefly explained below. For each $\underline{\mathcal{X}}_{k-1}^i$ from the input collection, we construct a collection $\mathcal{C}_k^i$ of constrained zonotopes, the union of which is contained by $Pre(\underline{\mathcal{X}}_{k-1}^i)$. To obtain $\mathcal{C}_k^i$, we compute a set $\mathcal{Z}_k^i$ of the state-input pairs $[\boldsymbol{x}; \boldsymbol{u}]$ using linearization (lines 2-5). These steps are the same as those in the scaling method except that the linearization error set $\mathcal{L}$ is now defined by a prescribed error bound $\bar{\boldsymbol{L}}$. If all possible values of the linearization error over $\mathcal{Z}_k^i$ are contained by $\mathcal{L}$, it follows that $Proj_{\boldsymbol{x}}(\mathcal{Z}_k^i) \cap \mathcal{X}_{\text{safe}} \subseteq Pre(\underline{\mathcal{X}}_{k-1}^i)$ and $\mathcal{C}_k^i$ is given as in line 7. Otherwise we split $\underline{\mathcal{X}}_{k-1}^i$ into two smaller constrained zonotopes $\underline{\mathcal{X}}_{k-1,1}^{i,j^*}$, $\underline{\mathcal{X}}_{k-1,2}^{i,j^*}$ and compute the BRSs for them by calling SplittingBRS recursively. Note that, for the first case (i.e., line 7), each $\mathcal{C}_k^i$ may still contain multiple sets when $\mathcal{X}_{\text{safe}}$ is nonconvex. For example, if $\mathcal{X}_{\text{safe}} = \bigcup_p \mathcal{H}_p$ is the union of finitely many polytopes $\mathcal{H}_p$, the collection $\mathcal{C}_k^i$ will consist of $Proj_{\boldsymbol{x}}(\mathcal{Z}_k^i) \cap \mathcal{H}_p$ for all p. Each $Proj_{\boldsymbol{x}}(\mathcal{Z}_k^i) \cap \mathcal{H}_p$ is a constrained zonotope, whose CG-Rep can be obtained by Lemma 1. For details, see [18]. Finally, if $\boldsymbol{f}$ is twice continuously differentiable, $LE(\boldsymbol{z}^*, \boldsymbol{f}, \mathcal{Z})$ will converge to a singleton set as $\mathcal{Z}$ does. This ensures that the recursion will terminate after sufficiently many splittings.

Algorithm 2 $\{\underline{\mathcal{X}}_k^\ell\}$ = SplittingBRS($\{\underline{\mathcal{X}}_{k-1}^i\}, \boldsymbol{f}, \mathcal{U}, \mathcal{W}, \bar{\boldsymbol{L}}, \mathcal{X}_{\text{safe}}$)

Input: A collection $\{\underline{\mathcal{X}}_{k-1}^i\}$ of constrained zonotopes; System's vector field $\boldsymbol{f}$; Control input set $\mathcal{U}$; Disturbance set $\mathcal{W}$; Safe set $\mathcal{X}_{\text{safe}}$; Admissible linearization error $\bar{\boldsymbol{L}} \in \mathbb{R}^n$

Output: A collection $\{\underline{\mathcal{X}}_k^\ell\}$ of constrained zonotopes s.t. $\bigcup_\ell \underline{\mathcal{X}}_k^\ell \subseteq Pre(\bigcup_i \underline{\mathcal{X}}_{k-1}^i)$

1: **for** each $\mathcal{X}_{k-1}^i$ **do**
2: $\quad \boldsymbol{z}^* \leftarrow center(\underline{\mathcal{X}}_{k-1}^i \times \mathcal{U})$
3: $\quad [\boldsymbol{A}, \boldsymbol{B}] \leftarrow linearize(\boldsymbol{z}^*, \boldsymbol{f})$
4: $\quad \mathcal{L} \leftarrow \langle \text{diag}(\bar{\boldsymbol{L}}), \boldsymbol{f}(\boldsymbol{z}^*) - [\boldsymbol{A}, \boldsymbol{B}]\boldsymbol{z}^* \rangle$
5: $\quad \mathcal{Z}_k^i \leftarrow Pre_{\boldsymbol{x},\boldsymbol{u}}(\underline{\mathcal{X}}_{k-1}^i, \boldsymbol{A}, \boldsymbol{B}, \mathcal{U}, \mathcal{W}, \mathcal{L})$
6: $\quad$ **if** $LE(\boldsymbol{z}^*, \boldsymbol{f}, \mathcal{Z}_k^i) \subseteq \mathcal{L}$ **then**
7: $\quad\quad \mathcal{C}_k^i \leftarrow \{Proj_{\boldsymbol{x}}(\mathcal{Z}_k^i) \cap \mathcal{X}_{\text{safe}}\}$
8: $\quad\quad$ **break**
9: $\quad$ **else**
10: $\quad\quad$ Select a generator $\boldsymbol{g}_{k-1}^{i,j^*}$ of $\underline{\mathcal{X}}_{k-1}^i$
11: $\quad\quad$ Split $\underline{\mathcal{X}}_{k-1}^i$ into $\underline{\mathcal{X}}_{k-1,1}^{i,j^*}$ and $\underline{\mathcal{X}}_{k-1,2}^{i,j^*}$ {Proposition 9}
12: $\quad\quad \mathcal{C}_{k-1}^i \leftarrow \{\underline{\mathcal{X}}_{k-1,1}^{i,j^*}, \underline{\mathcal{X}}_{k-1,2}^{i,j^*}\}$
13: $\quad\quad \mathcal{C}_k^i \leftarrow$ SplittingBRS($\mathcal{C}_{k-1}^i, \boldsymbol{f}, \mathcal{U}, \mathcal{W}, \bar{\boldsymbol{L}}, \mathcal{X}_{\text{safe}}$)
14: **return** $\{\underline{\mathcal{X}}_k^\ell\} \leftarrow \bigcup_i \mathcal{C}_k^i$

In line 10, the generator $\boldsymbol{g}_{k-1}^{i,j^*}$ is selected as follows. Similar to [25], for the j^{th} generator of the set $\underline{\mathcal{X}}_{k-1}^i$ to split, we compute a performance index ρ_j as follows:

$$\rho_j = \max(\boldsymbol{L}_1^j / \bar{\boldsymbol{L}}) \cdot \max(\boldsymbol{L}_2^j / \bar{\boldsymbol{L}}), \tag{54}$$

where $\boldsymbol{L}_1^j$, $\boldsymbol{L}_2^j \in \mathbb{R}^n$ are vectors that define the linearization error bound for sets $\mathcal{X}_{k,1}^{i,j}$ and $\mathcal{X}_{k,2}^{i,j}$, respectively. The operations max and / in Eq. (54) are element-wise. In line 10, the generator $\boldsymbol{g}_{k-1}^{i,j^*}$ with the lowest performance index will be chosen, i.e., $j^* = \arg\min_j \rho_j$.

Remark 6. Note that, while executing SplittingBRS in line 13, the set $\mathcal{L} \oplus \mathcal{W}$ will be subtracted from the two sets $\underline{\mathcal{X}}_{k-1,1}^{i,j^*}$ and $\underline{\mathcal{X}}_{k-1,2}^{i,j^*}$, which are obtained via splitting. By Lemma 2, bullet iii), the union of these two Minkowski differences is only a subset of (but not necessarily equal to) $\underline{\mathcal{X}}_{k-1}^i \ominus (\mathcal{L} \oplus \mathcal{W})$. This means that the splitting procedure introduces more conservatism. However, the overlapping area generated by Proposition 9 can ease the conservatism. This is because the larger $\underline{\mathcal{X}}_{k-1,1}^{i,j^*}$ and $\underline{\mathcal{X}}_{k-1,2}^{i,j^*}$ are, the larger $\mathcal{C}_k^i$ is.

When doing the splitting, the number of the obtained constrained zonotopes may grow exponentially. Therefore, a sampling algorithm is required to restrict their number. In order to evenly cover the union of these sets, we implement the farthest point sampling algorithm [26] based on the geometric centers of the constrained zonotopes' interval closures.

VII. Examples

In this section we illustrate our algorithms with several examples. TABLE I summarizes our results with, for each example and method, the system dimension d, the iteration steps k and the computing time. These examples were run on a laptop with a 12th generation Intel CPU and 16 GB of RAM. Our implementation is in MATLAB R2019a. The zonotope-based method and the HJB method that we use as benchmarks are also in MATLAB. Note that the splitting method does not apply to Example 2 because the system is linear and $\mathcal{X}_{\text{safe}}$ is convex (hence no reason for splitting). We also do not apply the scaling methods to examples with nonconvex $\mathcal{X}_{\text{safe}}$ (Examples 4 and 5), because its implementation only generates one homotopy class.

	d	k	Splitting	Scaling	HJB
Example 2	2	100	N/A	56.1s	45.2s
Example 3	10	10	226.7s	N/A	Memory error
Example 4: Convex constraints	3	–	478.9s ($k = 25$)	2821.3s ($k = 400$)	Memory error
Example 4: Nonconvex constraints	3	20	1564.1s	N/A	4521.6s
Example 5	10	340	951.6s	N/A	Memory error

TABLE I. Computation time for the examples.

While Algorithm 1, 2 are developed for nonlinear systems, they both reduce to Eq. (4) for linear systems (i.e., when $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{u}) = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{B}\boldsymbol{u}$). The following linear system examples show that less conservative under-approximations can be obtained using constrained zonotopes instead of zonotopes, because the former has a stronger expressive power.

Example 2. Consider a linear system with the following system matrices and sets:

$$\boldsymbol{A} = \begin{bmatrix} 0.9962 & 0.02394 \\ -0.1496 & 0.9962 \end{bmatrix}, \boldsymbol{B} = \begin{bmatrix} -0.004034 \\ 0.08025 \end{bmatrix}, \tag{55}$$

$\mathcal{U} = [\![-1.5, 1.5]\!]$, $\mathcal{W} = \langle [0.1997, 0.002396; -0.01498, 0.1997], \boldsymbol{0} \rangle$, $\mathcal{X}_0 = \langle \text{diag}([0.5, 0.5]), [1.5; 0] \rangle$ and $\mathcal{X}_{\text{safe}} = \{x \in \mathbb{R}^2 \mid [-1, 0; 2, 1]x \leq [2; 5]\}$. Fig. 3 shows the exact BRSs $\mathcal{X}_k$ (gray) for $k = 1, 2 \ldots, 100$ and their under-approximations. The constrained zonotopic under-approximations $\underline{\mathcal{X}}_k$ are in

	Exact	Constrained zonotope	Zonotope	HJB
Volume	37.079	28.343	7.810	2.817

TABLE II. EXAMPLE 2, THE VOLUME OF THE BRSS.

	Constrained zonotope	HJB	Intersection
Volume	0.1608	0.3422	0.1504
Projection Volume	0.7070	0.7326	0.6674

TABLE III. EXAMPLE 4, THE VOLUME OF THE BRSS AND THEIR PROJECTIONS.

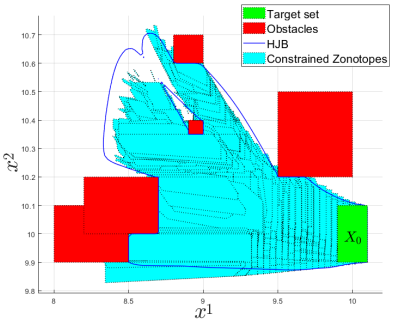

Fig. 5. Example 4 (nonconvex state constraints), BRSs by the splitting method.

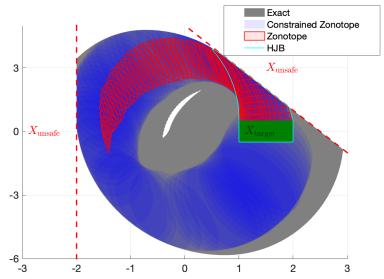

Fig. 3. Example 2, exact BRSs and their under-approximations.

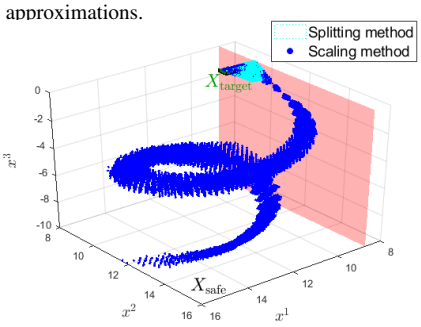

Fig. 6. Example 4 (convex constraints), BRSs by the scaling method and the splitting method.

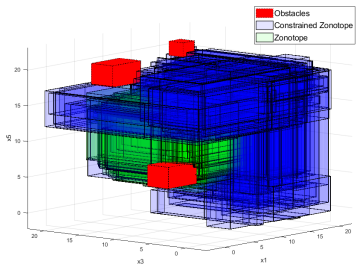

Fig. 4. Example 3, BRSs by the zonotope-based & the constrained-zonotope-based methods.

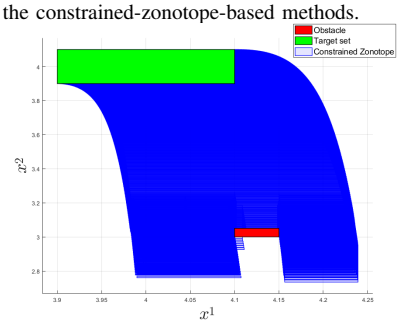

Fig. 7. Example 5, the projections of the 10-D BRSs.

blue. As a comparison, we used the method in [19] to compute zonotopic under-approximations (red) and scaled the generators of these zonotopes to satisfy the linear safety constraints. The latter approach is clearly more conservative (i.e., gives smaller sets). In fact, due to the wrapping effect after hitting the unsafe set $\{\boldsymbol{x} \mid [2,1]\boldsymbol{x} > 5\}$, the red sets vanish before $k = 100$ is reached. The main reason of this conservatism is that the true backward reachable set $\mathcal{X}_k$ becomes asymmetric due to the state constraints. Hence it is more accurate to approximate $\mathcal{X}_k$ with a constrained zonotope than with a zonotope. The former is as expressive as polytopes while the latter is restricted to be a centrally symmetric set.

In addition, we use the HJB method to compute the BRSs (cyan contour) with the same constraints. The obtained result is more conservative and stops expanding after $k = 20$. The volumes of the BRSs by different methods are approximated using a sample-based method and are shown in TABLE II.

Example 3. Consider the 10-D system from [19], discretized with a sampling period of $\Delta t = 0.1$s. Let the disturbance set $\mathcal{W}$ be so that $w_{\{1,3,5\}} \in [\![-0.12, 0.12]\!]$, $w_{\{2,4,6\}} \in [\![-0.2, 0.2]\!]$, $w_{\{7,8,9,10\}} \in [\![-0.1, 0.1]\!]$ and the control set $\mathcal{U} \in [\![-0.5, 0.5]\!]^3$. Define the target set such that $x_i \in [\![9.5, 10.5]\!]$ for $i \in \{1,2,3,4,5,6\}$ and $x_i \in [\![8, 12]\!]$ for $i \in \{7,8,9,10\}$.

To avoid potential numerical issues when visualizing 10-D zonotopes or constrained zonotopes, bounding boxes are used to visualize the results. Fig. 4 shows the 3-D projection of the boxes including the constrained zonotopic under-approximation of BRSs (blue) and zonotopic under-approximation of BRSs (green) for $k = 1, 2 \cdots, 10$. Since the system dimension is large, Hamilton-Jacobi method encountered memory error, whereas both zonotope and constrained zonotope-based methods can obtain a result. Here we used the approach in Sec. VI-B to avoid obstacles. In this example, the zonotopic representation is more conservative than that based on constrained zonotopes, while the latter being as scalable as the former. That is, constrained zonotopes can also handle high dimensional linear systems, as zonotopes do.

Example 4. Consider a Dubins Car system: $x^1_{k+1} = x^1_k + u^1_k \cos(x^3_k)$, $x^2_{k+1} = x^2_k + u^1_k \sin(x^3_k)$, $x^3_{k+1} = x^3_k + u^2_k$, where $\boldsymbol{x}_k = [x^1_k; x^2_k; x^3_k]$ is the state and $\boldsymbol{u}_k = [u^1_k; u^2_k] \in [\![0.04, 0.08]\!] \times [\![0, 0.04]\!]$ is the control input. We use the scaling method and the splitting method to compute the BRSs with convex and nonconvex state constraints, respectively.

Fig. 5 shows the $[x^1; x^2]$-projection of the constrained zonotopic under-approximation $\underline{\mathcal{X}}_k$ (cyan) of the BRSs, obtained by the splitting method. As a comparison, we also use the HJB method [22] to approximate the BRSs (blue contour). To this end, a uniform grid ($201 \times 201 \times 101$) of the state space is used. The BRSs obtained via these two methods both contain states from different homotopy classes in an environment with obstacles. Further, the two methods give BRSs that are similar in sizes but not comparable in the set inclusion sense (Fig 5 & TABLE III). In particular, when expanding into the free state space, the HJB method tends to give larger BRSs than the splitting method. However, the splitting method is faster (TABLE I). The volumes of the BRSs (and their projections) obtained using both methods are approximated using a sample-based method and are shown in TABLE III.

Fig. 6 shows $\underline{\mathcal{X}}_k$ obtained by the scaling method (blue) and the splitting method (cyan). Here the safe set is a single half-space (specified by the red plane). For small k's, the splitting method finds larger BRSs than the scaling method. However, the splitting method has difficulties to proceed for $k \geq 25$.

This is because, in the splitting method, $\underline{\mathcal{X}}_k$ is represented as a collection of small sets, whose number grows fast without an obstacle "pruning" these sets in a convex domain. It is also conservative to Minkowski subtract $\mathcal{L} \oplus \mathcal{W}$ from each small set in the collection, and uses the union of the obtained Minkowski-differences to compute $\underline{\mathcal{X}}_{k+1}$ (see Remark 6). On the contrary, the scaling method, which computes one set at each step, does not suffer from these issues and can compute the BRSs in a convex domain for a longer time horizon.

Example 5. Consider a 10-D water tank system with the following dynamics: $x^1_{k+1} = x^1_k + dt\big(u - k_2 x^{10}_k - k_1\sqrt{2gx^1_k}\big)$, $x^i_{k+1} = x^i_k + dtk_1\Big(\sqrt{2gx^{i-1}_k} - \sqrt{2gx^i_k}\Big)$ for $i \neq 1$, where x^i is the i^{th} tank's water level, $u \in [\![0.135, 0.145]\!]$ is the inflow, $dt = 0.01$, $k_1 = 0.015$, $k_2 = 0.01$, $g = 9.81$, and the target set is $[\![3.9, 4.1]\!]^{10}$. We apply the splitting method to this example. Figure 7 shows the 2-D projections of the target set (green), the obstacle (red), and the bounding boxes (blue) that include the obtained constrained zonotopic under-approximations of the BRSs. For this example, the HJB toolbox reports a memory error due to the large grid size, which is necessary for the 10-D system. We manage to compute the BRSs (with two homotopy classes) in reasonable time (TABLE I). This example shows that our method can deal with high-dimensional nonlinear systems with nonconvex state constraints.

VIII. Conclusion & Future Work

In this paper, we developed constrained-zonotope-based methods to under-approximate the BRSs for discrete-time nonlinear systems. Our main technical contribution was twofold. First, we developed an efficient way to under-approximate the Minkowski difference between a constrained zonotopic minuend and a zonotopic subtrahend, which is a necessary step in the sequential BRS computation. Our under-approximation was shown to be exact for minuends with rich enough CG-Reps. Secondly, using the developed Minkowski difference computation technique, we proposed two methods, i.e., the scaling method and the splitting method, for BRS computation. Experiments showed that these constrained-zonotope-based methods were less conservative than those using zonotopes, and were more scalable than the HJB method.

The exactness result in Sec. V suggests that, for constrained zonotopes, there is a trade-off between the computational complexity and the accuracy of set operations. This trade-off may be better understood via a systematic conversion between the different CG-Reps of a constrained zonotope. This conversion may be used, e.g., to incrementally enrich the CG-Rep of a constrained zonotopic minuend and improve our two-step approach's accuracy. We will explore this in the future.

References

[1] D. Bertsekas and I. Rhodes, "On the minimax reachability of target sets and target tubes," *Automatica*, vol. 7, no. 2, pp. 233–247, 1971.

[2] J. Lygeros, C. Tomlin, and S. Sastry, "Controllers for reachability specifications for hybrid systems," *Automatica*, vol. 35, no. 3, pp. 349–370, 1999.

[3] D. Bertsekas, "Infinite time reachability of state-space regions by using feedback control," *IEEE TAC*, vol. 17, no. 5, pp. 604–613, 1972.

[4] I. M. Mitchell, "Comparing forward and backward reachability as tools for safety analysis," in *Intl. Workshop on HSCC*. Springer, 2007, pp. 428–443.

[5] M. Chen, Q. Tam, S. C. Livingston, and M. Pavone, "Signal temporal logic meets reachability: Connections and applications," in *Intl. WAFR*. Springer, 2018, pp. 581–601.

[6] G. Chou, Y. E. Sahin, L. Yang, K. J. Rutledge, P. Nilsson, and N. Ozay, "Using control synthesis to generate corner cases: A case study on autonomous driving," *IEEE TCAD*, vol. 37, no. 11, pp. 2906–2917, 2018.

[7] L. Yang and N. Ozay, "Synthesis-guided adversarial scenario generation for gray-box feedback control systems with sensing imperfections," *ACM TECS*, vol. 20, no. 5s, pp. 1–25, 2021.

[8] E. Goubault and S. Putot, "Inner and outer reachability for the verification of control systems," in *Proc. of the 22nd HSCC*, 2019, pp. 11–22.

[9] B. Schurmann, M. Klischat, N. Kochdumper, and M. Althoff, "Formal safety net control using backward reachability analysis," *IEEE TAC*, 2021.

[10] M. Althoff, G. Frehse, and A. Girard, "Set propagation techniques for reachability analysis," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 4, pp. 369–395, 2021.

[11] X. Chen, S. Sankaranarayanan, and E. Ábrahám, "Under-approximate flowpipes for non-linear continuous systems," in *2014 FMCAD*. IEEE, 2014, pp. 59–66.

[12] N. Kochdumper and M. Althoff, "Computing non-convex inner-approximations of reachable sets for nonlinear continuous systems," in *the 59th CDC*. IEEE, 2020, pp. 2130–2137.

[13] E. Hnyilicza, "A set-theoretic approach to state estimation," Master's thesis, Massachusetts Institute of Technology, 1969.

[14] I. Kolmanovsky and E. G. Gilbert, "Theory and computation of disturbance invariant sets for discrete-time linear systems," *Mathematical Problems in Engineering*, vol. 4, no. 4, pp. 317–367, 1998.

[15] H. R. Tiwary, "On the hardness of computing intersection, union and minkowski sum of polytopes," *Discrete & Computational Geometry*, vol. 40, no. 3, pp. 469–479, 2008.

[16] M. Herceg, M. Kvasnica, C. Jones, and M. Morari, "Multi-Parametric Toolbox 3.0," in *Proc. of the 12th ECC*, 2013, pp. 502–510.

[17] M. Althoff, "On computing the minkowski difference of zonotopes," *arXiv preprint arXiv:1512.02794*, 2015.

[18] V. Raghuraman and J. P. Koeln, "Set operations and order reductions for constrained zonotopes," *Automatica*, vol. 139, p. 110204, 2022.

[19] L. Yang and N. Ozay, "Scalable zonotopic under-approximation of backward reachable sets for uncertain linear systems," *IEEE L-CSS*, vol. 6, pp. 1555–1560, 2021.

[20] S. Sadraddini and R. Tedrake, "Linear encodings for polytope containment problems," in *the 58th CDC*. IEEE, 2019, pp. 4367–4372.

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

[22] S. Bansal, M. Chen, S. Herbert, and C. J. Tomlin, "Hamilton-jacobi reachability: A brief overview and recent advances," in *the 56th CDC*. IEEE, 2017, pp. 2242–2253.

[23] A. Kulmburg and M. Althoff, "On the co-np-completeness of the zonotope containment problem," *Eur. J. Control*, vol. 62, pp. 84–91, 2021.

[24] M. Althoff, "Reachability analysis of nonlinear systems using conservative polynomialization and non-convex sets," in *Proc. of the 16th HSCC*, 2013, pp. 173–182.

[25] M. Althoff, O. Stursberg, and M. Buss, "Reachability analysis of nonlinear systems with uncertain parameters using conservative linearization," in *the 47th CDC*. IEEE, 2008, pp. 4042–4048.

[26] T. F. Gonzalez, "Clustering to minimize the maximum intercluster distance," *Theoretical computer science*, vol. 38, pp. 293–306, 1985.