An enhanced hierarchy for (robust) controlled invariance

Tzanis Anevlavis* Zexiang Liu* Necmiye Ozay Paulo Tabuada

Abstract— **We revisit the problem of computing controlled invariant sets for controllable discrete-time linear systems. Inspired by previous work by the authors, our main idea works in two moves: the problem is lifted to a higher dimensional space, where we provide a closed-form expression for a set whose projection back onto the original space is proven to be controlled invariant. We propose two methods, in which the key insight is computing controlled invariant sets by considering periodic control policies. The first method considers hyper-boxes that are rendered recurrent and essentially improves computational performance of the authors' previous work, while computing the same sets. The second method relaxes the assumption of recurrent hyper-boxes and yields substantially larger controlled invariant sets as shown in case studies. These methods do not rely on iterative computations and their scalability is illustrated in several examples, which show that none of the methods is strictly better than the other.**

I. Introduction

The problem of computing Controlled Invariant Sets (CIS) is the technical problem to be solved when synthesizing a controller enforcing safety properties. By definition, any trajectory starting in a CIS can be forced to remain therein by a choice of admissible control inputs. If a trajectory is to remain indefinitely in a set of safe states, then the initial condition must be contained in a CIS within the set of safe states. Consequently, CISs possess a central role in several control design problems, e.g., they act as safe sets in constrained control [7], [12], guarantee feasibility of optimization problems in Model Predictive Control (MPC) [11], [14], and more recently used in controller synthesis for safety properties expressed in temporal logic [19], [21], [23].

As a result, a substantial effort has been devoted to computing CISs. Beginning with the pioneering work of [5] on the computation of the *Maximal* Controlled Invariant Set (MCIS), many contributions followed and are documented in [6]. However, the method in [5] is not guaranteed to terminate in general and it does not scale well with the system's dimension. To alleviate the computational burden, alternative approaches have been investigated. Some of the state-of-the-art methods propose inner and outer approximations of the MCIS by solving optimization problems [13], [20], [24]. Naturally, outer approximations are not invariant, but even inner approximations are not guaranteed to be. A different approach [18] computes enlarged controlled λ-contractive sets, but requires knowledge of an existing λ-contractive set. Other works study cases where termination of the classical algorithm is guaranteed, such as controllable discrete-time linear systems, with states and inputs in finite unions of hyper-boxes [23], [26], and the case of bounded perturbations, with states and inputs in polytopes [22].

In the same spirit, [1], [2], [16] compute *exact*, as opposed to approximate, CISs and guarantee finite termination. In [16], an efficient method for computing ellipsoidal CISs for a class of hybrid systems is presented, and [1] discusses a novel method for the class of controllable discrete-time linear systems. The approach in [1] lifts the problem to a higher dimensional space, where the set of safe states is represented by a union of hyper-boxes. In this space, the MCIS is computed as a union of invariant hyper-boxes. Under the lens of automata theory, where a set of states is invariant if and only if it contains a loop [17], the more general problem of constructing recurrent hyper-boxes is solved in [2] and a *hierarchy* is established based on the loop length. Both [1], [2] compute a CIS in a higher dimensional space in closed-form and then project it back to the original space, where it is still invariant. Hence, their bottleneck is the projection from the higher dimensional space to the original space.

Inspired by the results in [1], [2], we propose two novel parameterizations for the CIS computed in the higher dimensional space. The contribution of this work is three-fold:

1) a parameterization of the CIS as a sequence of recurrent hyper-boxes using periodic control policies. This result is equivalent to [2], but offers significantly reduced computation time, as it lifts to smaller spaces than before;
2) a novel parameterization for the CIS by constraints on both states and inputs, under fixed periodic control policies, which provides considerably less conservative CISs;
3) a generalization of the results to systems with bounded disturbances, leading to *Robust* Controlled Invariant Sets.

A similar idea using recurrent sets is explored in [15] in the context of MPC. The goal there is to find *positively invariant* terminal sets for the closed-loop system, whereas we study existence and computation of *controlled invariant* sets.

Our simulations suggest that the second method is overall better in terms of computation time, but there exist cases where the first one is faster. Thus, if the goal is efficiency the faster method is prefered. However, if the criterion is the size of the CIS, then the second approach is always preferred.

This work was supported in part by the NSF grant 1645824, the CONIX Research Center, one of six centers in JUMP, a Semiconductor Research Corporation (SRC) program sponsored by DARPA, the NSF grant ECCS-1553873, and by the Automotive Research Center, a US Army Center of Excellence for modeling and simulation of ground vehicles, led by the University of Michigan under agreement W56HZV-19-2-0001. DISTRIBUTION A. Approved for public release; distribution unlimited. (OPSEC 4166)

T. Anevlavis and P. Tabuada are with the UCLA Electrical and Computer Engineering Department, Los Angeles, CA 90095 {janis10, tabuada} @ucla.edu. Z. Liu and N. Ozay are with the Dept. of Electrical Engineering and Computer Science, Univ. of Michigan, Ann Arbor, MI 48109, USA {zexiang, necmiye} @umich.edu.

* *T. Anevlavis and Z. Liu are co-first authors.*

The paper is organized as follows, in Section II the problem is mathematically set up, along with the essential definitions. Next, Section III briefly recalls the ideas of [1], [2], and provides the main technical results. Section IV provides a thorough computational evaluation of the proposed methods, prior to concluding our remarks in Section V.

II. Problem formulation and Preliminaries

We begin with the necessary definitions. This work focuses on controllable linear systems, and therefore we work with the Brunovsky normal form [8] of a linear system. Any controllable linear system can be transformed in this form by a suitable change of coordinates and state feedback [3].

Definition 1 (Discrete-time linear system): A *Discrete-Time Linear System* (DTLS) Σ, in the Brunovsky normal form, is a linear difference equation:

$$x^{+}=\begin{bmatrix}0 & 1 & \cdots & 0\\ \vdots & & \ddots & \vdots\\ 0 & \cdots & \cdots & 1\\ 0 & \cdots & \cdots & 0\end{bmatrix}x+\begin{bmatrix}0\\ \vdots\\ 0\\ 1\end{bmatrix}u+w=Ax+Bu+w, \quad (1)$$

where $x \in \mathbb{R}^n$ is the state of the system, $u \in \mathbb{R}$ is the input, $w \in W \subset \mathbb{R}^n$ is a disturbance term, $A \in \mathbb{R}^{n\times n}$, and $B \in \mathbb{R}^n$. By defining $u \in \mathbb{R}$, we implicitly consider single-input systems (see Remark 2 for multi-input systems).

Definition 2 (Polytope): A *polytope* S in $\mathbb{R}^n$ is a bounded set of the form:

$$S = \{x \in \mathbb{R}^n \mid Gx \leq f\}, \quad (2)$$

where $G \in \mathbb{R}^{K\times n}$, and $f \in \mathbb{R}^K$.

Assumption 1: The following *assumptions* are part of the problem setup:

1) The pair (A, B) in system Σ is controllable[1].
2) The set $S \subset \mathbb{R}^n$ is a polytope. We call S the *safe set*.
3) The disturbance set W is a polytope.

Definition 3 (Controlled invariant set): Given a polytope S and a DTLS Σ, a set $\mathcal{C} \subseteq S$ is a *Robust Controlled Invariant Set* (RCIS) of S for Σ if:

$$x \in \mathcal{C} \Rightarrow \exists u \in \mathbb{R} \text{ such that } \forall w \in W : Ax + Bu + w \in \mathcal{C}.$$

Given two sets $P, Q \subseteq \mathbb{R}^n$, denote their Minkowski sum by $P + Q = \{p + q \mid p \in P, q \in Q\}$, and their Minkowsky difference by $Q - P = \{x \in \mathbb{R}^n | x + P \subseteq Q\}$. By slightly abusing the notation, denote the Minkowsky sum of a singleton $\{x\}$ and a set P by $x + P$.

Define the *controlled predecessor* of a set $X \subset \mathbb{R}^n$ for the DTLS Σ as:

$$\mathrm{Pre}_\Sigma(X) = \{x \in \mathbb{R}^n \mid \exists u \in \mathbb{R}, Ax + Bu + W \subseteq X\}.$$

Intuitively, $\mathrm{Pre}_\Sigma(X)$ maps a set X to the set of all states $x \in \mathbb{R}^n$, for which there exists a control input v forcing them into X in one time-step, robustly to any disturbance in W. Next, define the *reachable set* from a set $X \subseteq \mathbb{R}^n$ under input sequence $\{u_i\}_{i=0}^{t-1}$ for a DTLS Σ as:

$$\mathcal{R}_\Sigma\left(X, \{u_i\}_{i=0}^{t-1}\right) = A^t X + \sum_{i=1}^{t} A^{i-1}Bu_{t-i} + \sum_{i=1}^{t} A^{i-1}W.$$

[1]This assumption is only used to obtain the Brunovsky normal form in (1). For details refer to [3, Ch. 3]

Intuitively, $\mathcal{R}_\Sigma\left(X, \{u_i\}_{i=0}^{t-1}\right)$ maps a set X and an input sequence $\{u_i\}_{i=0}^{t-1}$ to the set of all states reachable from X in t steps, by applying the input sequence $\{u_i\}_{i=0}^{t-1}$. By definition, if $\mathcal{R}_\Sigma(X, u) \subseteq Y$ for some u, then $X \subseteq \mathrm{Pre}_\Sigma(Y)$. Conventionally, $\mathcal{R}_\Sigma(X, \emptyset) = X$.

Remark 1 (Input constraints): To ease notation, we assume unconstrained inputs, i.e., $u \in \mathbb{R}$. To impose input constraints, $u \in \mathcal{U} \subset \mathbb{R}$, one extends the state as $y = (x, u)$, and introduces a new unconstrained input $\nu \in \mathbb{R}$ governing the evolution of the state u as $u^+ = \nu$. The input constraints are now part of the extended system's safe set $S \times \mathcal{U} \subset \mathbb{R}^n \times \mathbb{R}$.

Remark 2 (The multi-input case): In this paper, we only discuss single-input systems to simplify the presentation. Using similar arguments, the same results can be generalized to controllable multi-input DTLSs.

III. Controlled invariance in higher dimensional spaces

The classical algorithm [5] that computes the MCIS uses an iterative procedure based on the Pre operator, and does not scale well with the system dimension. As a remedy, two promising techniques were developed in [1], [2] based on an idea working in two moves: 1) lift the safe set S and the DTLS Σ to a higher dimensional space, where the MCIS of the lifted set and system is computed in closed-form; 2) project the computed MCIS back to the original space to obtain a CIS for the original problem.

Step 1 is computationally efficient as a closed-form expression is provided. In contrast, step 2 requires a projection, which is a costly operation [10] as the dimensionality gap between the lifted and the original space can be large. Consequently, the bottleneck of the above idea lies in step 2. Naturally, the question of how to rectify this issue arises.

The main objective of this paper is to provide more efficient alternatives that compute at least the same CIS as in [1], [2], but with lower complexity.

A. Controlled invariance in two moves

In [1], the safe set S in (2) is represented as a union of hyper-boxes by introducing a variable $\lambda \in \mathbb{R}^{Kn}$, where K is the number of facets in S. Then, $S \subset \mathbb{R}^n$ is *lifted* to $S^\ell \subset \mathbb{R}^{n+Kn}$ as follows:

$$\begin{cases} g_{ji}x_i \leq \lambda_i^j, i = 1, \cdots, n \\ \sum_{i=1}^n \lambda_i^j \leq f_j \end{cases}, \ j = 1, \ldots, K, \quad (3)$$

where x_i is the i-th coordinate of $x \in \mathbb{R}^n$, g_{ji} is the entry corresponding to the j-th row and i-th column of G, and $\lambda = \left(\lambda^1, \ldots, \lambda^k\right) \in \mathbb{R}^{Kn}$, $\lambda^j \in \mathbb{R}^n$, $j = 1, \ldots, K$. Hence, the problem is lifted from $\mathbb{R}^n$ to $\mathbb{R}^{n+Kn}$, where the MCIS is computed exactly in closed-form [1, Th. 3.1]. This MCIS can be interpreted as a union of invariant hyper-boxes.

Based on the lift in (3), a *hierarchy* of CISs is proposed in [2]. The key idea is to relax invariant hyper-boxes to recurrent hyper-boxes with period L, which is the decision parameter. By increasing L, one potentially obtains larger CISs (see [2, Sec. 4.6]). The problem is lifted from $\mathbb{R}^n$ to $\mathbb{R}^{n+LKn}$, where the MCIS is computed exactly in closed-form [2, Sec. 7].

B. A more efficient hierarchy (Method 1)

To provide more efficient methods, we provide an alternative definition of recurrent hyper-boxes.

Definition 4 (L-invariant set): Given $L \in \mathbb{N}^+$, we call a hyper-box $B_0 \subseteq S$ *L-invariant* with respect to Σ, if there exist $L-1$ hyper-boxes $B_1 \ldots, B_{L-1} \subseteq S$, satisfying:

$$B_{\mathrm{mod}(t,L)} \subseteq \mathrm{Pre}_\Sigma\left(B_{\mathrm{mod}(t+1,L)}\right), t = 0, \ldots, L-1. \quad (4)$$

It follows that any B_t in the sequence is L-invariant, and $\cup_{t=0}^{L-1} B_t \subseteq S$ is an RCIS. Define now the following problem.

Problem 1: Given a safe set $S \subset \mathbb{R}^n$, and a system Σ in Brunovsky normal form with disturbance set $W \subset \mathbb{R}^n$, find all L-invariant hyper-boxes in S with respect to Σ.

Denote by $\mathcal{B}(L)$, the set of all L-invariant hyper-boxes. It follows then, that:

$$C_{\mathcal{B},L} = \bigcup_{B \in \mathcal{B}(L)} B, \quad (5)$$

is an RCIS by construction. While [2] provides the exact solution to Problem 1, [1] offers the solution for $L = 1$. Here we provide a more efficient solution to Problem 1.

Proposition 3.1: The set $C_{\mathcal{B},L}$ in (5) is unchanged if the disturbance set W of system Σ is replaced by the smallest hyper-box $W_B = \Pi_{i=1}^n [\underline{w}_i, \overline{w}_i] = [\underline{w}, \overline{w}]$ that contains W.

Proof: Denote the system with disturbance set W_B by Σ'. For any hyper-boxes B_1 and B_2, it can be shown that $B_1 \subseteq \mathrm{Pre}_\Sigma(B_2)$ if and only if $B_1 \subseteq \mathrm{Pre}_{\Sigma'}(B_2)$. Thus, by definition, any L-invariant hyper-box with respect to Σ is also L-invariant with respect to Σ'. ■

Remark 3: According to Proposition 3.1, we use W_B instead of W to simplify technical results, for the remainder of this subsection, without introducing extra conservativeness.

We propose an equivalent, but more efficient, lift to (3). Define a hyper-box $B = \Pi_{i=1}^n \left[\underline{b}_i, \overline{b}_i\right]$. An equivalent set of conditions to (3) describing any hyper-box $B \subseteq S$, is:

$$\sum_{i=1}^n g_{ji}\left(\frac{1-\mathrm{sgn}(g_{ji})}{2}\underline{b}_i + \frac{1+\mathrm{sgn}(g_{ji})}{2}\overline{b}_i\right) \leq f_j, \quad j = 1, \ldots, K. \quad (6)$$

Construction (6) lifts $\mathbb{R}^n$ to $\mathbb{R}^{n+2n}$, which is of lower dimension compared to $\mathbb{R}^{n+Kn}$ from (3), immediately improving the implementations in [1], [2].

Given any two hyper-boxes, the next Proposition describes conditions under which $\mathrm{Pre}_\Sigma(\cdot)$ of one contains the other.

Proposition 3.2: Given any $B_1 = \Pi_{i=1}^n \left[\underline{b}_{1,i}, \overline{b}_{1,i}\right]$ and $B_2 = \Pi_{i=1}^n \left[\underline{b}_{2,i}, \overline{b}_{2,i}\right]$, we have $B_1 \subseteq \mathrm{Pre}_\Sigma(B_2)$ if and only if: (1) $u \in \left[\underline{b}_{2,n}, \overline{b}_{2,n}\right] - \left[\underline{w}_n, \overline{w}_n\right] \neq \emptyset$; and (2) for any $u \in \left[\underline{b}_{2,n}, \overline{b}_{2,n}\right] - \left[\underline{w}_n, \overline{w}_n\right] \neq \emptyset$, $\mathcal{R}_\Sigma(B_1, u) \subseteq B_2$.

Proof: For any $x = (x_1, x_2, \ldots, x_n) \in B_1$, we have $x_i \in \left[\underline{b}_{1,i}, \overline{b}_{1,i}\right]$, $i = 1, \ldots, n$, and the next state can be written as $x^+ = (x_2 + w_1, \ldots, x_n + w_{n-1}, u + w_n)$. Simple calculations show that $B_1 \subseteq \mathrm{Pre}_\Sigma(B_2) \Leftrightarrow \exists u \in \mathbb{R}$, such that $\mathcal{R}_\Sigma(x, u) = Ax + Bu + W \subseteq B_2 \Leftrightarrow$ the following holds:

$$\left[\underline{b}_{1,i+1}, \overline{b}_{1,i+1}\right] + \left[\underline{w}_i, \overline{w}_i\right] \subseteq \left[\underline{b}_{2,i}, \overline{b}_{2,i}\right], i = 1, \ldots, n-1,$$
$$\left[\underline{b}_{2,n}, \overline{b}_{2,n}\right] - \left[\underline{w}_n, \overline{w}_n\right] \neq \emptyset,$$

and $u \in \left[\underline{b}_{2,n}, \overline{b}_{2,n}\right] - \left[\underline{w}_n, \overline{w}_n\right] \Rightarrow \mathcal{R}_\Sigma(B_1, u) \subseteq B_2$. ■

We now provide the main theorem of this subsection.

Theorem 3.3: Consider a safe set $S \subset \mathbb{R}^n$ and a DTLS Σ, for which Assumption 1 holds. The *robust controlled invariant* set $C_{\mathcal{B},L}$ defined in (5), is given by:

$$C_{\mathcal{B},L} = \pi_{\mathbb{R}^n}(S_{\mathcal{B},L}), \quad (7)$$

where $S_{\mathcal{B},L}$ is the set of points $(x, l, u, u_0, \ldots, u_{L-1})$ satisfying:

$$x \in B_0 \equiv \Pi_{i=1}^n \left[\underline{b}_i, \overline{b}_i\right] \subseteq S, \quad (8)$$
$$\mathcal{R}_\Sigma(B_0, \{u_i\}_{i=0}^{t-1}) \subseteq S, \; t = 1, \ldots, L-1, \quad (9)$$
$$\mathcal{R}_\Sigma(B_0, \{u_i\}_{i=0}^{L-1}) \subseteq B_0. \quad (10)$$

See Appendix A for the closed-form expression of $S_{\mathcal{B},L}$ as a polytope in $\mathbb{R}^{3n+L}$.

Proof: We first show that $B_0 \subseteq S$ is L-invariant $\Leftrightarrow$ $\exists u_0, u_1, \ldots, u_{L-1} \in \mathbb{R}$ satisfying:

$$\mathcal{R}_\Sigma\left(B_0, \{u_i\}_{i=0}^{t-1}\right) \subseteq S, \; t = 0, \ldots, L-1 \quad (11)$$
$$\mathcal{R}_\Sigma\left(B_0, \{u_i\}_{i=0}^{L-1}\right) \subseteq B. \quad (12)$$

$B_0 \subseteq S$ is L-invariant $\overset{\text{Def. 4}}{\Longleftrightarrow}$ $\exists B_t \subseteq S$, $t = 1, \ldots, L-1$, s.t. $B_{\mathrm{mod}(t,L)} \subseteq \mathrm{Pre}_\Sigma\left(B_{\mathrm{mod}(t+1,L)}\right)$ $\overset{\text{Prop. 3.2}}{\Longleftrightarrow}$ $\exists u_t \in \mathbb{R}$ s.t. $\mathcal{R}_\Sigma\left(B_{\mathrm{mod}(t,L)}, u_t\right) \subseteq B_{\mathrm{mod}(t+1,L)}$, $t = 0, \ldots, L-1$.

Define $B_t = \mathcal{R}_\Sigma(B_{t-1}, u_{t-1}) = AB_{t-1} + Bu_{t-1} + W_B$, $t = 1, \ldots, L-1$, which are hyper-boxes since W_B is a box, then (11), (12) follow.

Consequently, the union of all L-invariant hyper-boxes $B_0 \subseteq S$ for system Σ is the set of states x satisfying the constraints in (8), (9), (10), computed by projecting $S_{\mathcal{B},L}$ onto the first n coordinates. ■

We can conclude from Theorem 3.3 and its proof, that if $C_{\mathcal{B},L}$ is non-empty, then there must exist a sequence of periodic inputs forcing any state in B, to loop back to B in L steps, while remaining in $C_{\mathcal{B},L}$ and consequently in the safe set. This is shown in Figure 1. Notice here that the L-invariant hyper-boxes computed as part of the solution by Method 1 keep their "box" shape despite the presence of disturbances. This can be especially helpful in high dimensional problems, where even polyhedral constraints give little intuition about the shapes of the sets and thus hyper-boxes are preferred.

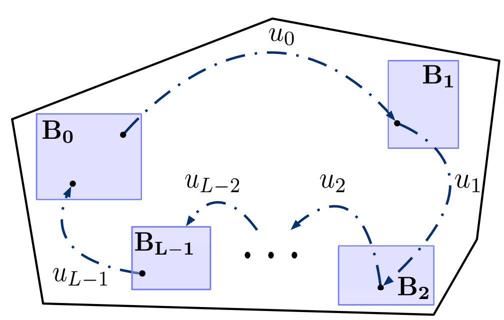

Fig. 1: Illustration of a sequence of L-invariant hyper-boxes, in blue, and the corresponding input sequence.

C. A less conservative hierarchy (Method 2)

So far, we essentially computed hyper-boxes rendered L-invariant by periodic inputs. This suggests that we may parameterize an RCIS by constraints on the states and on a sequence of periodic inputs. Any such state $x \in S$ satisfies:

$$\exists \{u_i\}_{i=0}^{t-1} \;:\; \mathcal{R}_\Sigma \left(x, \{u_{\mathrm{mod}(i,L)}\}_{i=0}^{t-1}\right) \subseteq S,\; t \geq 0, \quad (13)$$

i.e., the reachable set from x, under the periodic control policy $u_t = u_{\mathrm{mod}(t,L)}$, remains in the safe set S. Notice that (13) defines an infinite number of constraints in general. However, under the above periodic policy they are reduced to a set of finite constraints as we show below. The system Σ is in Brunovsky normal form and, hence, we have that:

$$\mathcal{R}_\Sigma\left(x, \{u_i\}_{i=0}^{t-1}\right) = A^\tau x + \sum_{i=1}^{\tau} A^{i-1} B u_{t-i} + \sum_{i=1}^{\tau} A^{i-1} W, \quad (14)$$

where $\tau = \min(t, n)$, since $A^t = 0$, for $t \geq n$. In light of (14), the constraints in (13) are separated as:

$$\mathcal{R}_\Sigma\left(x, \{u_{\mathrm{mod}(i,L)}\}_{i=0}^{t-1}\right) \subseteq S,\; t = 0, \ldots, n-1, \quad (15)$$

$$\mathcal{R}_\Sigma\left(\{u_{\mathrm{mod}(i,L)}\}_{i=0}^{t-1}\right) \subseteq S,\; t \geq n, \quad (16)$$

where in (16) we omit x as it is independent of x given (14). Due to the cyclic nature of u, we observe from (14) that the constraints in (16) repeat as t increases:

$$u_{\mathrm{mod}(i,L)} = u_{\mathrm{mod}(i+kL,L)},\; k \in \mathbb{N}$$
$$\Rightarrow \mathcal{R}_\Sigma\left(\{u_{\mathrm{mod}(i,L)}\}_{i=0}^{t-1}\right) = \mathcal{R}_\Sigma\left(\{u_{\mathrm{mod}(i,L)}\}_{i=0}^{t+kL-1}\right),\; t \geq n.$$

Thus, (16) is equivalent to:

$$\mathcal{R}_\Sigma\left(\{u_{\mathrm{mod}(i,L)}\}_{i=0}^{t-1}\right) \subseteq S, t = n, \ldots, n+L-1. \quad (17)$$

Consequently, we have shown that under the periodic policy $u_t = u_{\mathrm{mod}(t,L)}$, the infinite number of constraints in (13) is reduced to a finite number of constraints in (15) and (17). These constraints define a set in the space of states x and input sequences $u_{\mathcal{L}} = (u_0, \ldots, u_{L-1}) \in \mathbb{R}^L$ as:

$$S_{\mathcal{U},L} = \left\{(x, u_{\mathcal{L}}) \in \mathbb{R}^{n+L} \middle| (x, u_{\mathcal{L}}) \text{ satisfy (15), (17)}\right\}, \quad (18)$$

which is a polytope given in closed-form in Appendix B. By projecting $S_{\mathcal{U},L}$ onto the first n coordinates, we obtain $C_{\mathcal{U},L} = \pi_{\mathbb{R}^n}(S_{\mathcal{U},L})$, which is an RCIS by construction. This can be understood as any state in a trajectory starting in $C_{\mathcal{U},L}$, can always be forced to stay in the safe set by a periodic input sequence and, therefore, is itself contained in $C_{\mathcal{U},L}$. The above is summarized in the following result.

Theorem 3.4: Consider a safe set $S \subset \mathbb{R}^n$ and a DTLS Σ, for which Assumption 1 holds. The set:

$$C_{\mathcal{U},L} = \pi_{\mathbb{R}^n}(S_{\mathcal{U},L}). \quad (19)$$

is *controlled invariant*, where $S_{\mathcal{U},L}$ is a polytope in $\mathbb{R}^{n+L}$, provided in closed-form in Appendix B.

Notice here that, similarly to [1] and [2], we can construct auxiliary higher dimensional systems for which $S_{\mathcal{B},L}$ and $S_{\mathcal{U},L}$ are controlled invariant.

Remark 4 (Complexity analysis): Method 1 amounts to projecting a polytope with $LK + 4n$ constraints from $\mathbb{R}^{n+2n+L}$ to $\mathbb{R}^n$, and Method 2 to projecting a polytope from R^{n+L} onto $\mathbb{R}^n$. The above is readily verified by the respective closed-form expressions in Appendices A and B. The improvement over [2], which requires projecting a polytope with an upper bound of $\frac{1}{2}n(n+1)K + LK + L\frac{(Kn)^2}{4}$ on its constraints from $\mathbb{R}^{n+LKn}$ to $\mathbb{R}^n$, is substantial. That is, the proposed methods scale better with L and K, i.e., larger loops and more complex safe sets.

TABLE I: Example 1: Execution time and CIS volume as the length of the loop L increases. System dimension $n = 5$.

		$L=1$	$L=2$	$L=3$	$L=4$	$L=5$
Mth. 1	Time (sec.)	0.99	0.71	2.08	5.82	318.9
	% of MCIS volume	0.75	1.26	1.80	3.59	5.78
Mth. 2	Time (sec.)	0.10	0.24	1.52	4.72	22.6
	% of MCIS volume	82.18	91.08	93.96	95.93	96.90
Alg. [2]	Time (sec.)	13.4	32.1	551.1	~ 3000	≥ 3600
	% of MCIS volume	0.75	1.26	1.80	3.59	5.78

Remark 5 (Conservativeness): Notice that $C_{\mathcal{U},L} \supseteq C_{\mathcal{B},L}$ in general. Moreover, Method 2 exploits the shape of W to compute an RCIS that is less conservative in terms of the disturbance effect, in contrast to Method 1, for which using W_B instead of W bears no difference, see Remark 3.

Corollary 3.5 (Correctness and completeness): If the sets computed by $C_{\mathcal{B},L}$ and $C_{\mathcal{U},L}$ are non-empty, then they are *controlled invariant* by construction. In the absence of disturbance, i.e., $W = \emptyset$, if the MCIS of S is non-empty, then $C_{\mathcal{B},L}$ is the same as the set in [2], and completeness of [2, Th. 4.3] implies completeness of Method 1. Moreover, $C_{\mathcal{U},L} \supseteq C_{\mathcal{B},L}$, which implies completeness of Method 2. When $W \neq \emptyset$, Methods 1 and 2 are not complete, see Section IV for a counter-example.

IV. Computational Evaluation

In this section, we perform a computational evaluation[2,3] of the proposed methods.

Example 1: Consider a continuous-time model for a truck with N trailers [23] in Fig. 2. The state is $x = (d_1, \ldots, d_N, u_0, \ldots, u_N)$ and, hence, N trailers correspond to dimension $n = 2N + 1$. The input is the velocity of the truck. We discretize the model with a sampling time of T_s seconds assuming piecewise constant inputs.

We illustrate how the proposed methods scale with the system dimension n and the loop length L on the above example. We compare to their predecessor [2], the method [16] that computes ellipsoidal CISs, and the `invariantSet()`

[2]The relevant code is available at: https://github.com/janis10/cis2m.

[3]Instructions and exact parameters of the examples are found at: https://github.com/janis10/cis2m/tree/master/paper-archive/ACC21.

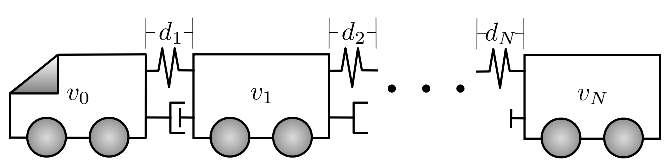

Fig. 2: Illustration of a truck with N trailers.

TABLE II: Example 1: CIS volume as the system dimension, $n = 2N + 1$, increases with the number of trailers N.

		$n = 3$	$n = 5$	$n = 7$	$n = 9$
Mth. 1 $L = 2$	Time (sec.)	0.33	0.75	2.78	33.19
	% of MCIS volume	91.81	1.26	NA	NA
Mth. 2 $L = 2$	Time (sec.)	0.07	0.25	1.12	145.02
	% of MCIS volume	96.38	91.07	NA	NA
Alg. [2] $L = 2$	Time (sec.)	3.01	33.41	259.1	~ 3200
	% of MCIS volume	91.81	1.26	NA	NA
Alg. [16]	Time (sec.)	0.07	0.11	0.13	0.17
	% of MCIS volume	4.64	0.32	NA	NA
MPT3 100 iterations	Time (sec.)	1.06	4.52	~ 1400	≥ 3600
	MCIS volume	21.68	20.75	NA	NA

function of the Multi-Parametric Toolbox (MPT3) [9], which computes the MCIS using the iterative procedure [5]. MPT3 is more costly computationally for higher dimensions, and therefore we set an upper bound of 100 iterations.

In Table I, we fix $n = 5$ and compare the runtimes of Methods 1, 2, and [2], as we increase L to obtain larger CISs. Both Methods 1 and 2 scale much better with L compared to [2]. Moreover, Method 2 computes less conservative CISs.

In Table II, we fix $L = 2$ and compare Methods 1, 2, [2], [16], and MPT3, as we increase n. The algorithm in [16] is the fastest, with Method 2 following close. Be that as it may, comparing the volumes of the computed CISs, reveals that the proposed methods return considerably larger sets, especially Method 2, and now much faster than before. Computing the MCIS using MPT3, although fairly quick for $n = 3, 5$, fails to converge in 100 iterations for larger values of n, and simulations were aborted, thus the computed set at that time is not a CIS. Notice, that we do not report volumes for $n = 7, 9$, since (1) MPT3 did not terminate and the MCIS is not obtained; and (2) we noticed that MPT3 function that computes the volume of a polytope was unstable in high dimensions.

It is worth noticing that virtually the entire runtime for our methods is consumed in projecting from the lifted space to the original space. By increasing L, the lifted space is larger, and in turn projection requires more effort [10]. Consequently, there is a trade-off between size of the CIS and execution time. Furthermore, in most cases Method 2 is faster than Method 1 as the lifted space of Method 2 is smaller than that of Method 1. However, in Table II, Method 2 is slower for the case $n = 9$. That is due to projection time being largely affected by the number of constraints of the projected polytope. For said case, $S_{\mathcal{U},L}$ has more constraints, $K(n + L)$, than the $(KL + 4n)$ of $S_{\mathcal{B},L}$. Thus, though our results support that Method 2 is typically faster, we cannot conclude that it is superior to Method 1 in terms of runtime.

Example 2: Consider the continuous-time lateral dynamics of a vehicle [25], with 4 states and constrained input, resulting in a system of $n = 5$ states and unconstrained input. We discretize the model with a sampling time of T_s seconds assuming piecewise constant inputs.

Table III shows how the size of the computed RCIS shrinks with increasing disturbance. As the disturbance bounds increase, our computed RCISs become empty, while the MRCIS is still non-empty. This serves as a counter-example disproving completeness of our methods in presence of disturbance. Finally, Table IV compares the proposed methods in absence of disturbances. The results resemble Table I, however in this case Method 1 performs considerably better as L increases. Moreover, even in the presence of input constraints, Method 2 quickly computes a sufficiently large part of the MCIS. As a comparison, MPT3 computes the MCIS in 9 seconds, whereas our method computes 95% of it, in just 0.41 seconds, i.e., almost 22 times faster.

For reference, the simulations were conducted on an iMac (Late 2012), 4-core Intel Core i7 Processor@3.4GHz and 32GB 1600MHz DDR3 RAM using MPT3 and MOSEK [4].

V. Discussion & Conclusion

In this paper, we presented two methods for computing RCISs that significantly improve performance over [1], [2]. Both methods offer substantially smaller computational overhead with respect to their predecessors. The first method reformulates the same ideas, but results in lifts to smaller spaces than before, which alleviates to some extent the bottleneck of projection. The second method generalizes the first and, thus, is able to compute even larger RCISs. Both methods still embody the idea of a hierarchy of RCISs. Increasing the loop length potentially yields larger RCISs, which introduces a trade-off between quality, i.e., size of the RCIS, and performance, i.e., runtime. Consequently, they render the proposed hierarchy even more useful for the practitioner.

TABLE III: Example 2: Performance of Method 2 when computing an RCIS as the disturbance, r_d, bounds grow.

	$\lvert r_d \rvert \leq$	0.005	0.010	0.015	0.020
Mth. 1 $L = 4$	% of MRCIS volume	2.59	0	0	0
Mth. 2 $L = 4$	% of MRCIS volume	95.41	88.83	64.31	0
MPT3	MRCIS volume	0.1935	0.1915	0.1895	0.1874

TABLE IV: Example 2: Execution time and CIS volume as the loop length L increases. No disturbance.

		$L = 2$	$L = 3$	$L = 4$	$L = 5$	$L = 6$
Mth. 1	Time (sec.)	0.72	0.87	1.65	19.94	241.9
	% of MCIS volume	3.15	5.69	11.6	20.1	30.6
Mth. 2	Time (sec.)	0.41	0.96	2.47	9.40	18.25
	% of MCIS volume	95.7	96.2	96.9	97.7	98.6

APPENDIX

A. Closed-form expression of $S_{\mathcal{B},L}$

Consider boxes $B_0 = \left[\underline{b}, \overline{b}\right], W_B = [\underline{w}, \overline{w}] \subset \mathbb{R}^n$. We show that (8), (9), (10) define a polytope given in closed-form.

1) Constraints (8), i.e., $x \in B_0$ and $B_0 \subseteq S$, described in (6), are immediately linear on $(x, \underline{b}, \overline{b})$.

2) Constraints (9), i.e., $\mathcal{R}_\Sigma\left(B_0, \{u_i\}_{i=0}^{t-1}\right) \subseteq S$ can be written as:

$$A^t B_0 + \sum_{i=1}^{t} A^{i-1} B u_{\mathrm{mod}(t-i,L)} + \sum_{i=1}^{t} A^t W_B \subseteq S.$$

The set on the lefthand side above is still a box, as both B_0 and W_B are boxes. Therefore, in the same manner as in (6), the above constraints are linear on $(\underline{b}, \overline{b}, u_0, \ldots, u_{L-1})$.

3) Constraints (10), i.e., $\mathcal{R}_\Sigma\left(B_0, \{u_i\}_{i=0}^{L-1}\right) \subseteq B_0$ can be written as:

$$A^{L-1} B_0 + \sum_{i=1}^{L=1} A^{i-1} B u_{\mathrm{mod}(t-i,L)} + \sum_{i=1}^{L-1} A^t W_B \subseteq B.$$

Similarly, the set on the lefthand side above is a box and the above constraints are linear on $(\underline{b}, \overline{b}, u_0, \ldots, u_{L-1})$.

Finally, $S_{\mathcal{B},L}$ is the polytope defined by constraints 1), 2), and 3) above, which are linear in $\left(x, \underline{b}, \overline{b}, u_0, \ldots, u_{L-1}\right) \in \mathbb{R}^{n+2n+L}$.

B. Closed-form expression of $S_{\mathcal{U},L}$

The set $S_{\mathcal{U},L}$ is the set of points $(x, u_0, \ldots, u_{L-1}) \in \mathbb{R}^{n+L}$ that satisfy constraints (15) and (17). These constraints, given (14), are respectively written as:

$$A^t x + \sum_{i=1}^{t} A^{i-1} B u_{\mathrm{mod}(t-i,L)} \subseteq S - \sum_{i=1}^{t} A^{i-1} W, \qquad t = 0, \ldots, n-1,$$

$$\sum_{i=1}^{n} A^{i-1} B u_{\mathrm{mod}(t-i,L)} \subseteq S - \sum_{i=1}^{n} A^{i-1} W, \qquad t = n, \ldots, n+L-1.$$

Since S and W are polytopes, then $S - \sum_{i=1}^{t} A^{i-1} W$, for $t = 1, \ldots, n$, are polytopes defined as a Minkowski difference. Therefore, the above constraints can be written as linear inequalities in $(x, u_0, \ldots, u_{L-1}) \in \mathbb{R}^{n+L}$ and define the polytope $S_{\mathcal{U},L}$.

REFERENCES

[1] T. Anevlavis and P. Tabuada, "Computing controlled invariant sets in two moves," in *2019 IEEE 58th Conference on Decision and Control (CDC)*, 2019, pp. 6248–6254. [Online]. Available: https://doi.org/10.1109/CDC40024.2019.9029610

[2] T. Anevlavis and P. Tabuada, "A simple hierarchy for computing controlled invariant sets," in *Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control*, ser. HSCC '20. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi.org/10.1145/3365365.3382205

[3] P. J. Antsaklis and A. Michel, *Linear Systems*, 1st ed. Birkhäuser Basel, 2006.

[4] M. ApS, *The MOSEK optimization toolbox for MATLAB manual. Version 8.1.0.75.*, 2019. [Online]. Available: http://docs.mosek.com/8.1/toolbox/index.html

[5] D. Bertsekas, "Infinite time reachability of state-space regions by using feedback control," *Automatic Control, IEEE Transactions on*, vol. AC-17, pp. 604 – 613, 11 1972.

[6] F. Blanchini and S. Miani, *Set–Theoretic Methods in Control*, ser. Systems & Control: Foundations & Applications. Boston, Basel, Berlin: Birkhauser, 2008.

[7] F. Borrelli, *Constrained Optimal Control of Linear and Hybrid Systems*, ser. Lecture Notes in Control and Information Sciences. Springer Berlin Heidelberg, 2003.

[8] P. Brunovský, "A classification of linear controllable systems," *Kybernetika*, vol. 6, pp. 173–188, 1970.

[9] M. Herceg, M. Kvasnica, C. Jones, and M. Morari, "Multi-Parametric Toolbox 3.0," in *Proc. of the European Control Conference*, Zürich, Switzerland, July 17–19 2013, pp. 502–510, http://control.ee.ethz.ch/ mpt.

[10] C. N. Jones, E. C. Kerrigan, and J. M. Maciejowski, "On polyhedral projection and parametric programming," *Journal of Optimization Theory and Applications*, vol. 138, no. 2, pp. 207–220, Aug 2008. [Online]. Available: https://doi.org/10.1007/s10957-008-9384-4

[11] E. C. Kerrigan and J. M. Maciejowski, "Invariant sets for constrained nonlinear discrete-time systems with application to feasibility in model predictive control," in *Proceedings of the 39th IEEE Conference on Decision and Control (Cat. No.00CH37187)*, vol. 5, Dec 2000, pp. 4951–4956 vol.5.

[12] E. Kerrigan, "Robust constraint satisfaction: Invariant sets and predictive control," *Ph.D. dissertation*, 10 2011.

[13] M. Korda, D. Henrion, and C. N. Jones, "Convex computation of the maximum controlled invariant set for polynomial control systems," *SIAM Journal on Control and Optimization*, vol. 52, no. 5, pp. 2944–2969, 2014. [Online]. Available: https://doi.org/10.1137/130914565

[14] M. Lazar, "Model predictive control of hybrid systems : stability and robustness," Ph.D. dissertation, Department of Electrical Engineering, 2006.

[15] M. Lazar and V. Spinu, "Finite-step terminal ingredients for stabilizing model predictive control," *IFAC-PapersOnLine*, vol. 48, no. 23, pp. 9–15, 2015, 5th IFAC Conference on Nonlinear Model Predictive Control NMPC 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405896315025409

[16] B. Legat, P. Tabuada, and R. M. Jungers, "Computing controlled invariant sets for hybrid systems with applications to model-predictive control," in *6th IFAC Conference on Analysis and Design of Hybrid Systems, ADHS 2018, Oxford, UK, July 11-13, 2018*, 2018, pp. 193–198.

[17] Z. Manna and A. Pnueli, "A hierarchy of temporal properties," Stanford, CA, USA, Tech. Rep., 1987.

[18] S. Munir, M. Hovd, and S. Olaru, "Low complexity constrained control using higher degree lyapunov functions," *Automatica*, vol. 98, pp. 215 – 222, 2018.

[19] P. Nilsson, O. Hussien, A. Balkan, Y. Chen, A. D. Ames, J. W. Grizzle, N. Ozay, H. Peng, and P. Tabuada, "Correct-by-construction adaptive cruise control: Two approaches," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 4, pp. 1294–1307, July 2016.

[20] A. Oustry, M. Tacchi, and D. Henrion, "Inner approximations of the maximal positively invariant set for polynomial dynamical systems," *IEEE Control Systems Letters*, vol. 3, no. 3, pp. 733–738, July 2019.

[21] M. Rungger, M. Mazo, and P. Tabuada, "Scaling up controller synthesis for linear systems and safety specifications," in *2012 IEEE 51st IEEE Conference on Decision and Control (CDC)*, Dec 2012, pp. 7638–7643.

[22] M. Rungger and P. Tabuada, "Computing robust controlled invariant sets of linear systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 7, pp. 3665–3670, July 2017.

[23] M. Rungger, M. Mazo, Jr., and P. Tabuada, "Specification-guided controller synthesis for linear systems and safe linear-time temporal logic," in *Proceedings of the 16th International Conference on Hybrid Systems: Computation and Control*, ser. HSCC '13. New York, NY, USA: ACM, 2013, pp. 333–342.

[24] M. A. B. Sassi and A. Girard, "Controller synthesis for robust invariance of polynomial dynamical systems using linear programming," *Systems & Control Letters*, vol. 61, no. 4, pp. 506 – 512, 2012.

[25] S. W. Smith, P. Nilsson, and N. Ozay, "Interdependence quantification for compositional control synthesis with an application in vehicle safety systems," in *2016 IEEE 55th Conference on Decision and Control (CDC)*, Dec 2016, pp. 5700–5707.

[26] R. Vidal, S. Schaffert, J. Lygeros, and S. Sastry, "Controlled invariance of discrete time systems," in *Proceedings of the Third International Workshop on Hybrid Systems: Computation and Control*, ser. HSCC '00. London, UK, UK: Springer-Verlag, 2000, pp. 437–450.