An efficient approach to invariant computation of discrete time affine hybrid systems

Arvind Adimoolam and Thao Dang

Verimag, Grenoble, France
{santosh.adimoolam,thao.dang}@univ-grenoble-alpes.fr.

1 Introduction

One of the most important requirements in the design of embedded and cyber-physical systems is safety which can be roughly stated as the system never enters a bad state. Safety verification for such systems are known to be computationally challenging due to the complexity in the interactions between their heterogenous components with mixed (continuous and discrete) dynamics. In this paper, we focus on the problem of finding invariants for hybrid systems which are mathematical widely recognized as suitable for modelling embedded and cyber-physical systems. An invariant is a property that is satisfied in every state that the system can reach. Therefore a common approach for proving a safety property is to find an invariant that implies the safety property. Invariant computation has been studied extensively in the context of abstract interpretation for program analysis (see for example [**?**, 3, 5, 8, 21, 22] and the techniques developed for generating invariants of programs have been extended to hybrid systems [**?**, **?**, 4, 7, 15, 18, 20]. Barrier certificates [16] are closely related to invariants in the sense that they describe a boundary that the system starting from a given initial set will never cross to enter a region containing bad states. Another common approach to safety verification is to compute or over-approximate the reachable set of the system. Reachability computation techniques have been developed for continuous and hybrid systems, and many of such techniques are based on iterative approximation on a step-by-step basis and can be thought of as a set-based extension numerical integration. A major drawback of this approach, inherent to undecidability of general hybrid systems with non-trivial dynamics, is that such an iterative procedure may not terminate and thus can only be used for bounded-time safety properties (when the over-approximation error accumulation is not too serious that the safety can be decided). Invariant and barrier certificate based approaches by contrast consider conditions that invariants or barrier certificates should satisfy at any time. Although solving these conditions often involves fixed point computation, by exploiting the structure of the dynamics (such as eigen-structures of linear systems) one can derive meaningful conditions which can significantly reduce the number of iterations until convergence.

For discrete time affine hybrid systems, the eigenvectors of the products of linear matrices related to the affine dynamics of different subsystems can possibly capture some of the stable directions for the overall hybrid dynamics. As such, for invariant computation, template complex zonotopes have the advantage that they can include the possibly complex eigenvectors among the generators, while usual (real) zonotopes can not. In an

earlier work [1], numerically efficiently solvable conditions for computing a template complex zonotopic invariant subject to linear safety constraints were obtained for a limited class of hybrid systems, i.e., having uncontrolled switching. However, a formidable hurdle in extending the approach for more general affine hybrid systems, where switching is controlled by linear constraints, is that we have to handle the intersection of template complex zonotopes with the linear constraints. In this regard, template complex zonotopes share the drawback of usual zonotopes that these classes of sets are not closed under intersection with linear constraints.

In this paper, we circumvent this problem as follows. We observe that it is possible to compute or reasonably overapproximate the intersection of a template complex zonotope with a class of linear constraints, called subparallelotpic, by appropriately choosing the template of the complex zonotope. We use a slightly more general set representation, called augmented complex zonotope, with which the intersection operation can be succinctly presented. Then, we derive a numerically efficiently solvable sufficient condition for computing an augmented complex zonotopic invaraint satisfying linear safety constraints, for a discrete time affine hybrid system with subparallelotopic switching constraints and bounded additive disturbance input. The sufficient condition is expressed as a set of second order conic constraints. We also note that the class of sub-parallelotopic constraints that we consider are quite general and can be used in the specification of many examples of affine hybrid systems. To corroborate our approach by presenting the experimental results for three benchmark examples from literature.

Related work. Before continuing, we discuss the relation of our work with the existing works. For hybrid systems verification, convex polyhedra [6, 12], and their special classes such as zones [14], octagons [**?**], zonotopes [**?**] and tropical polyhedra [**?**] are the most commonly used set representations. During the analysis which requires operations under which a set representation is not closed (such as the union or join operations for convex polyhedra and additionally intersection for zonotopes) the complexity of generated sets increases rapidly in order to guarantee a desired error bound. One way to control this complexity increase, face normal vectors or generators are fixed, which led to template convex polyhedra [7, 19]. Although our template complex zonotopes proposed in [**?**] do not belong to the class of convex polyhedra, they follow the same spirit. Set representations defined by non-linear constraints include ellipsoids [**?**], polynomial inequalities [**?**] et equalities [**?**], quadratic templates and piecewise quadratic templates [**?**, **?**, **?**], which are used for computing non-linear invariants. A major problem that the template based approach faces is finding good templates. As it will become clear later, using template complex zonotopes and the augmented version introduced in this paper and exploiting eigen-structures of linear dynamics which reflects the contraction or expansion of a set by the dynamics, allows requiring only few of steps until convergence to an invariant.

The complex zonotopes we proposed in [**?**] extend usual zonotopes to the complex domain, and geometrically speaking they are Minkowski sum of line segments and some ellipsoids. This extension is very similar in spirit to quadratic zonotopes [**?**] and more generally polynomial zonotopes [**?**]. Nevertheless, while a polynomial zonotope is a set-valued polynomial function of *intervals*, a complex zonotope is a set-valued function of unit *circles* in the complex plane. Our idea of coupling additional linear

constraints with zonotopes is inspired by the work on constrained zonotopes proposed in [10] for intersection computation.

Organization. The rest of the paper is organized as follows. Firstly, we explain some of the mathematical notation used in this paper. Then in Section 2, we describe the model of a discrete time affine hybrid system, controlled by sub-parallelotopic switching conditions and having a bounded additive disturbance input. In Section **??**, we review some existing set representations before presenting augmented complex zonotopes. In Section 3, we present the set representaion of augmented complex zonotopes and discuss some important operations and relations like intersection with sub-parallelotopic constraints, projection in any direction, linear transformation, Minkowski sum and inclusion. In Section 4, we derive a set of second order conic constraints to compute an augmented complex zonotopic invariant, satisfying linear safety constraints and containing an initial set. Furthermore, we explain how to choose the template. In Section 5, we discuss the experimental results. The conclusion and future work are given in Section 6. We annex the proofs of the lemmas presented in the paper as an Appendix.

Notation. Some of the notations used in this paper, for which we consider explanation may be required, is described below. If S is a set of complex numbers, then $real(S)$ represents the real projection of S. If z is a complex number, then $|z|$ denotes the absolute value of z. On the other hand, if X is a complex matrix, then $|X|$ denotes the matrix containing the absolute values of the elements of X. The diagonal square matrix containing the entries of a complex vector z along the diagonal is denoted by $\mathcal{D}(z)$. Let $K \in \mathbb{M}_{k\times n}(\mathbb{R})$ such that $k \leq n$ and KK^T is non-singular. Then, we denote $K^\dagger = K^T \left(KK^T\right)^{-1}$, which is the pseudo-inverse of K. Given two vectors $l, u \in \mathbb{R}^k$, the meet of the two vectors is denoted $l \bigwedge u$, defined as $(l \bigwedge u)_i = \min(l_i, u_i)\ \forall i \in \{1, ..., k\}$. The join is denoted $l \bigvee u$, defined as $(l \bigvee u)_i = \max(l_i, u_i)\ \forall i \in \{1, ..., k\}$.

2 Hybrid systems and positive invariants

In a discrete-time affine hybrid system, we have a finite set of discrete variables, called locations, and a finite set of continuous variables whose valuation is in the real Euclidean space of dimension $n \in \mathbb{Z}_{>0}$. In each location, there are a set of linear constraints, called *staying conditions*, within which the continuous state of the system in that location is constrained. Furthermore, there is an affine transition map with (possibly) additive uncertain but bounded disturbance input specifying the evolution of the continuous variables. A set of labeled directed edges specify possible discrete transitions between locations, accompanied by affine reset map on continuous variables with a bounded additive disturbance input. Each edge transition is controlled by a set of linear constraints on the continuous variables, called guards.

In this paper, we consider a specific class of linear constraints called, sub-parallelotopic, for defining guards and staying conditions, such that their intersection with the reachable set represented by augmented complex zonotopes (introduced later) can be effectively computed. The sets corresponding to sub-parallelotopic constraints can be seen as a generalization of parallelotopes to possibly unbounded sets. We discuss the aforementioned intersection operation later after defining augmented complex zonotopes.

Definition 1 (Sub-parallelotope). *Let $K \in \mathbb{M}_{k\times n}(\mathbb{R})$ such that $k \leq n$ and $\left(KK^T\right)$ is non-singular. We call such a matrix K a* sub-parallelotopic template*. Let $\widehat{u}, \widehat{l} \in \overline{\mathbb{R}}^n$ such that $\widehat{u} \leq \widehat{l}$. Then the following is a sub-parallelotopic set.*

$$\mathcal{P}\left(K, \widehat{l}, \widehat{u}\right) = \left\{x \in \mathbb{R}^n : \widehat{l} \leq Kx \leq \widehat{u}\right\}$$

For example, the set of linear constraints $-1 \leq x + y - z \leq 1 \ \wedge \ \ x - y + z \leq 3$ is equivalent to a sub-parallelotope

$$\mathcal{P}\left(\begin{bmatrix} [1 & 1 & -1] \\ [1 & -1 & 1] \end{bmatrix}, \begin{bmatrix} -1 \\ -\infty \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \end{bmatrix}\right),$$

because the rows of the sub-parallelotopic template are linearly independent. On the other hand, the set of constraints $-1 \leq x+y-z \leq 1 \ \wedge \ x+y+z \leq 2 \wedge \ -1 \leq x+y$ do not constitute a sub-parallelotope, because the three row vectors $\begin{bmatrix} 1 & 1 & -1 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$, and $\begin{bmatrix} 1 & 1 & 0 \end{bmatrix}$ together are linearly dependent.

System model. We consider discrete-time affine hybrid systems defined by a tuple

$$\mathbb{H} = (Q, \mathcal{K}, \gamma, \mathcal{A}, U, E).$$

Here, Q is a finite set of locations. For each location $q \in Q$, a sub-parallelotopic template $\mathcal{K}_q \in \mathbb{M}_{k_q\times n}(\mathbb{R})$, i.e., $\mathcal{K}_q \left(\mathcal{K}_q\right)^T$ is non-singular, and $k(q)$ is the number of rows of the template, is used for defining the staying conditions and the guards on edges emanating from the location. Then, a pair of upper and lower bounds $\gamma_q = \left(\gamma_q^-, \gamma_q^+\right) \in \mathbb{R}^{k_q} \times \mathbb{R}^{k_q} \ : \ \ \gamma_q^- \leq \gamma_q^+$ together with the sub-parallelotopic template define the sub-parallelotopic staying set as $\mathcal{P}\left(\mathcal{K}_q, \gamma_q^-, \gamma_q^+\right)$. The matrix A_q and a bounded set $U_q \subseteq \mathbb{R}^n$ define the linear transformation and the additive input set in the location. The set of edges is E, where $\sigma \in E$ is a tuple $\sigma = (\sigma_1, \sigma_2, \sigma^-, \sigma^+, \Theta_\sigma, \Omega_\sigma)$. The pre and post locations of the edge are $\sigma_1 \in Q$ and $\sigma_2 \in Q$, respectively. The pair of upper and lower bounds $(\sigma^-, \sigma^+) \in \mathbb{R}^{k_{\sigma_1}} \times \mathbb{R}^{k_{\sigma_1}} : \ \sigma^- \leq \sigma^+$, gives the sub-parallelotopic guard set $\mathcal{P}\left(\mathcal{K}_{\sigma_1}, \sigma^-, \sigma^+\right)$, which is a precondition on the edge transition. The matrix Θ_σ and a bounded set $\Omega_\sigma \subseteq \mathbb{R}^n$, respectively, give the linear transfomation and the additive input set for all edge (interlocation) transitions.

Dynamics. The state of the hybrid system is a pair (x, q), where $x \in \mathbb{R}^n$ is called the continuous state and $q \in Q$ is called the discrete state. The evolution of the state of the system in time is called a *trajectory* of the system. The trajectory is a function $(\mathbf{x}, \mathbf{q}) : \mathbb{Z}_{\geq 0} \to \mathbb{R}^n \times Q$, such that for all $t \in \mathbb{Z}_{\geq 0}$, one of the following is true.

1. Intralocation dynamics.

$$\begin{aligned} &\exists u \in U_{\mathbf{q}(t)} \ \text{ such that all of the following are collectively true.} \\ &\mathbf{x}(t+1) = \mathcal{A}_{\mathbf{q}(t)}\mathbf{x}(t) + u, \quad \mathbf{q}(t+1) = \mathbf{q}(t) \ \text{ and} \\ &\mathbf{x}(t),\ \mathbf{x}(t+1) \in \mathcal{P}\left(\mathcal{K}_{\mathbf{q}(t)}, \gamma^-_{\mathbf{q}(t)}, \gamma^+_{\mathbf{q}(t)}\right). \end{aligned} \tag{1}$$

2. Interlocation dynamics.

$$\begin{aligned}
&\exists \sigma \in E \text{ and } u \in \Omega_\sigma \text{ such that all of the following are collectively true.} \\
&\mathbf{q}(t) = \sigma_1, \quad \mathbf{x}(t) \in \mathcal{P}\left(\mathcal{K}_{\sigma_1}, \sigma^- \bigvee \gamma^-_{\sigma_1}, \sigma^+ \bigwedge \gamma^+_{\sigma_1}\right) \\
&\mathbf{x}(t+1) = \Theta_{\mathbf{q}(t)}\mathbf{x}(t) + u, \quad \mathbf{q}(t+1) = \sigma_2 \\
&\mathbf{x}(t+1) \in \mathcal{P}\left(\mathcal{K}_{\sigma_2}, \gamma^-_{\sigma_2}, \gamma^+_{\sigma_2}\right).
\end{aligned} \tag{2}$$

Given a set of continuous states $S \in \mathbb{R}^n$, we compute the set of reachable continuous states in the next time step of intralocation transition in a location $q \in Q$ or interlocation transition along an edge $\sigma \in E$, by the functions $R_q : 2^{\mathbb{R}^n} \to 2^{\mathbb{R}^n}$ or $R_\sigma : 2^{\mathbb{R}^n} \to 2^{\mathbb{R}^n}$, respectively, defined as

$$R_q(S) = \begin{cases} \left(\mathcal{A}_q\left(S \bigcap \mathcal{P}\left(\mathcal{K}_q, \gamma^-_q, \gamma^+_q\right)\right) \oplus U_q\right) \\ \bigcap \ \mathcal{P}\left(\mathcal{K}_q, \gamma^-_q, \gamma^+_q\right) \end{cases}.$$

$$R_\sigma(S) = \begin{cases} \left(\Theta_\sigma\left(S \bigcap \mathcal{P}\left(\mathcal{K}_{\sigma_1}, \sigma^- \bigvee \gamma^-_{\sigma_1}, \sigma^+ \bigwedge \gamma^+_{\sigma_1}\right)\right) \oplus \Omega_\sigma\right) \\ \bigcap \ \mathcal{P}\left(\mathcal{K}_{\sigma_2}, \gamma^-_{\sigma_2}, \gamma^+_{\sigma_2}\right) \end{cases}.$$

We shall identify a set of states by a mapping of the kind $\Gamma : Q \to 2^{\mathbb{R}^n}$, called a *state set*, which corresponds to the set of states $\{(x, q) : x \in \Gamma(q)\}$. For notational convenience, we shall denote Γ_q as the set of continuous states of Γ in a location q. A *positive invariant* is a set of states of the system such that all trajectories beginning at any state in the positive invariant remain within the positive invariant. Equivalently, a state set is a positive invariant if the reachable set in one time step by both the intralocation and interlocation dynamics is contained within the original state set.

Definition 2. *A state set Γ is a positive invariant if the following is true.*

$$\forall q \in Q, \ \ R_q(\Gamma_q) \subseteq \Gamma_q \ \textit{ and } \ \forall \sigma \in E, \ \ R_\sigma(\Gamma_{\sigma_1}) \subseteq \Gamma_{\sigma_2}.$$

3 Augmented complex zonotopes

Before we introduce augmented complex zonotopes, we briefly review the related set representations that are used in this paper. Firstly, polytopes can be defined in terms of halfspace representation. Let $T \in \mathbb{M}_{n\times k}(\mathbb{R})$ and $d \in \mathbb{R}^k$. Then a (possibly unbounded) *polytope*, denoted $\mathcal{J}(T, d)$, is defined as $\mathcal{J}(T, d) = \left\{x \in \overline{\mathbb{R}}^k : Tx \leq d\right\}$. Usual zonotopes form a subclass of polytopes, which are geometrically Minkowski sums of line segments. They are represented as a linear combination of real vectors, called *generators*, whose combining coefficients are bounded in real valued intervals. Let $W \in \mathbb{M}_{n\times k}(\mathbb{R})$ and $l, u \in \mathbb{R}^m : l \leq u$. Then a *real zonotope* is $\mathcal{Z}(W, l, u) = \left\{W\zeta : \zeta \in \mathbb{R}^k, \ \zeta_i \in [l_i, u_i] \ \forall i \in \{1, ..., k\}\right\}$. For simple examples of zonotopes like boxes and octagons, efficient interconversion between the zonotopic representation and halfspace polytopic representation is possible. However, in general, zonotopes do not have efficient halfspace representation as a polytope. The reason is that a zonotope with

m generators in an n dimensional space has $\binom{m}{n}$ faces (bounding hyperplanes), if all combinations of n generators are linearly independent. That is, the halfspace representation of a zonotope can be exponentially large, compared to the above generator representation.
Zonotopes are closed under linear transformations and Minkowski sums, which can be computed efficiently. Hence, zonotopes are considered efficient for reachability analysis of linear systems. Nevertheless, a major drawback of zonotopes is that their intersection with sets defined by linear constraints need not be zonotopes. To incorporate the possibly complex (having real and imaginary parts) eigenstructure of linear maps while computing invariants, the complex zonotope set representation and its generalization to the template complex zontope were introduced in [1, 2]. A template complex zonotope has complex valued vectors as generators, whose combining coefficients are complex and bounded in their absolute values.

Definition 3 (Template complex zonotope). *Let $V \in \mathbb{M}_{n\times m}(\mathbb{C})$ (template) and $s \in \mathbb{R}^m_{\geq 0}$ (scaling factors) and $c \in \mathbb{R}^n$ (center). Then the following is a template complex zonotope: $\mathcal{C}(V, c, s) = \{V\epsilon : \epsilon \in \mathbb{C}^m,\ |\epsilon_i| \leq s_i\ \forall i \in \{1, ..., m\}\}$.*

Unlike real zonotopes, a template complex zonotope can have a non-polyhedral real projection. Therefore, in general, checking the exact inclusion between two template complex zonotopes amounts to solving a non-convex optimization problem, which could be computationally intractable. Instead, a convex condition was proposed in [1], which is sufficient to guarantee the inclusion between template complex zonotopes. Here, we present this condition as a relation between template complex zonotopes.

Definition 4. *We define a relation "$\sqsubseteq$" between template complex zonotopes as $\mathcal{C}\left(V'_{n\times m'}, c', s'\right) \sqsubseteq \mathcal{C}(V_{n\times m}, c, s)$ if all of the below statements are collectively true.*

$$\begin{aligned} &\exists X \in \mathbb{M}_{m\times m'}(\mathbb{C}) \text{ and } y \in \mathbb{C}^m \text{ s.t.} \\ &VX = V'\mathcal{D}(s'), \quad Vy = c' - c \\ &\max_{i=1}^{m} \left(|y_i| + \sum_{j=1}^{m'} |X_{ij}| - s_i \right) \leq 0 \end{aligned} \tag{3}$$

Lemma 1 (Inclusion: template complex zonotopes). *The inclusion $\mathcal{C}(V', c', s') \subseteq \mathcal{C}(V, c, s)$ holds if the relation $\mathcal{C}(V', c', s') \sqsubseteq \mathcal{C}(V, c, s)$ is true.*

Proof idea. We relate the combining coefficients of the two template complex zonotopes by a linear transformation, with appropriate bounds on the transformation matrix such that the inclusion holds.
For fixed V and V', we observe that (3) is equivalent to as a set of convex constraints called second order conic constraints. A second order conic constraint (SOCC) is defined as follows. A constraint of the form $\|Ax\|_2 + Fx + b \leq 0$ on an n-dimensional variable x, given $A, F \in \mathbb{M}_{n\times k}(\mathbb{R})$ and $b \in \mathbb{R}^k$, is a second order conic constraint. We also note that linear inequalities and equalities can be expressed in the form of SOCC described above. Our aforementioned observation about (3) is formalized below.

Proposition 1. *For fixed V,V', the relation $\mathcal{C}(V', c', s') \sqsubseteq \mathcal{C}(V, c, s)$ is equivalent to a set of second order conic constraints on the variables c, c', s, s', l, l' and some additional variables.*

There are many convex optimization tools that can efficiently solve SOCC upto a high numerical precision. An augmented complex zonotope is the Minkowski sum of a template complex zonotope and a real zonotope. In terms of expressivity, an augmented complex zonotope is slightly more general than template complex zonotopes. But geometrically, the sets that can be described as real projections of augmented complex zonotopes can also be described as real projections of template complex zonotopes. However, with augmented complex zonotopes, the intersection with subparallelotopic constraints can be succinctly specified, as we will see latter. Consequently, this representation is more convenient to derive conditions for computing invariants for the affine hybrid system.

Definition 5 (Augmented complex zonotope). *Let $V \in \mathbb{M}_{n\times m}(\mathbb{C})$ called primary template, $W \in \mathbb{M}_{n\times k}(\mathbb{R})$ called secondary template, $c \in \mathbb{R}^n$ called primary offset, $s \in \mathbb{R}^m$ called scaling factors, $u, l \in \mathbb{R}^k$ called lower and upper interval bounds, respectively, such that $l \leq u$. The following is an augmented complex zonotope.*

$$\mathcal{G}(V, c, s, W, l, u) = \mathcal{C}(V, c, s) \oplus \mathcal{Z}(W, l, u).$$

In invariant computation, we have to overapproximate the intersection between the augmented complex zonotope and sub-parallelotopic constraints. In this regard, we state the following Theorem that gives an overapproximation of the intersection between an augmented complex zonotope and a suitably aligned subparallelotope as another augmented complex zonotope. Furthermore, under an orthogonality condition stated below, we can compute the exact intersection.

Theorem 1. *Let $\mathcal{K}$ be a subparalleotopic template and $c \in \mathbb{C}^n$ such that $\mathcal{K}c = 0$. Then,*

1. $\mathcal{G}\left(V, c, s, \mathcal{K}^\dagger, l, u\right) \bigcap \mathcal{P}\left(\mathcal{K}, \widehat{l}, \widehat{u}\right) \subseteq \mathcal{G}\left(V, c, s, \mathcal{K}^\dagger, l \bigvee \widehat{l}, u \bigwedge \widehat{u}\right)$.
2. *If $\mathcal{K}V = 0$, then* $\mathcal{G}\left(V, c, s, \mathcal{K}^\dagger, l, u\right) \bigcap \mathcal{P}\left(\mathcal{K}, \widehat{l}, \widehat{u}\right) = \mathcal{G}\left(V, c, s, \mathcal{K}^\dagger, l \bigvee \widehat{l}, u \bigwedge \widehat{u}\right)$.

Proof. First we prove $\mathcal{G}\left(V, c, s, \mathcal{K}^\dagger, l, u\right) \bigcap \mathcal{P}\left(\mathcal{K}, \widehat{l}, \widehat{u}\right) \subseteq \mathcal{G}\left(V, c, s, \mathcal{K}^\dagger, l \bigvee \widehat{l}, u \bigwedge \widehat{u}\right)$, as follows. Let $x \in \mathcal{G}\left(V, c, s, \mathcal{K}^\dagger, l, u\right) \bigcap \mathcal{P}\left(\mathcal{K}, \widehat{l}, \widehat{u}\right)$. Then it can be written as $x = y + z$, s.t. $y \in \mathcal{C}(V, c, s)$ and $z \in \mathcal{Z}\left(\mathcal{K}, \widehat{l}, \widehat{u}\right)$.

Similar to usual zonotopes, augmented complex zonotopes are closed under Minkowski sums and linear transformations, and their computations are also similar. The computation of some important operations are summarized as follows.

1. $A\mathcal{G}(V, c, s, W, l, u) = \mathcal{G}(AV, Ac, s, AW, l, u)$.
2. $\mathcal{G}(V, c, s, W, l, u) \oplus \mathcal{G}(V', c', s', W', l', u')$
   $= \mathcal{G}\left(\left[V \;\; V'\right], c + c', \begin{bmatrix} s \\ s' \end{bmatrix}, \left[W \;\; W'\right], \begin{bmatrix} l \\ l' \end{bmatrix}, \begin{bmatrix} u \\ u' \end{bmatrix}\right)$

3. The limits of the projection of an augmented complex zonotope along any direction can be computed as follows. For $v \in \mathbb{R}^n$,

$$\max_{x \in \mathcal{G}(V,c,s,W,l,u)} v^T x = v^T \left(c + W \frac{l+u}{2} \right) + \left| v^T [V \;\; W] \right| \left(\begin{bmatrix} s \\ \frac{u-l}{2} \end{bmatrix} \right) \quad (4)$$

The real projection of an augmented complex zonotope can be equivalently transformed as the real projection of a template complex zonotope, as follows.

Lemma 2. $\mathrm{Re}\left(\mathcal{G}\left(V, c, s, W, l, u\right)\right) = \mathrm{Re}\left(\mathcal{C}\left(\left[V\ W\right], c + W\left(\frac{u+l}{2}\right), \begin{bmatrix} s \\ \frac{u-l}{2} \end{bmatrix}\right)\right)$.

Because of the above relationship, checking the inclusion between the real projections of two augmented complex zonotopes amounts to checking the inclusion between real projections of two template complex zonotopes. Recall the relation between template complex zonotopes that was a sufficient condition for inclusion. We extend the relation to augmented complex zonotopes as follows.

Definition 6. *We say that* $\mathcal{G}\left(V', c', s', W', l', u'\right) \sqsubseteq \mathcal{G}\left(V, c, s, W, l, u\right)$ *if* $\mathcal{C}\left(\left[V'\ W'\right], c' + W'\left(\frac{u'+l'}{2}\right), \begin{bmatrix} s' \\ \frac{u-l}{2} \end{bmatrix}\right) \sqsubseteq \mathcal{C}\left(\left[V\ W\right], c + W\left(\frac{u+l}{2}\right), \begin{bmatrix} s \\ \frac{u-l}{2} \end{bmatrix}\right)$.

Lemma 3 (Inclusion: augmented complex zonotopes). *The real inclusion* $\mathrm{Re}\left(\mathcal{G}\left(V', c', s', W', l', u'\right)\right) \subseteq \mathrm{Re}\left(\mathcal{G}\left(V, c, s, W_{n\times k}, l, u\right)\right)$ *holds if the relation* $\mathcal{G}\left(V', c', s', W', l', u'\right) \sqsubseteq \mathcal{G}\left(V, c, s, W_{n\times k}, l, u\right)$ *is true.*

The intersection of an augmented complex zonotope with a subparallelotope involves the meet and join operations, as stated in Lemma 1. These operations are piecewise affine functions of their arguments, but not affine. Hence, their composition with a convex function may be non-convex. But since we are interested in deriving convex conditions for finding an invariant, in this regard, we define the following upper and lower bound functions for the join and meet operations, respectively.

Let us define a binary function $\widehat{\Lambda} : \mathbb{R}^k \times \overline{\mathbb{R}}^k$, called *min-approximation* function, as follows. For $u \in \mathbb{R}^k$ and $\widehat{u} \in \overline{\mathbb{R}}^k$, $\left(\widehat{\Lambda}\left(u, \widehat{u}\right)\right)_i = \begin{cases} \widehat{u}_i & \text{if } \widehat{u}_i < \inf \\ u_i & \text{if } \widehat{u}_i = \inf \end{cases}$. Similarly, let us define another binary function $\overline{\Lambda} : \mathbb{R}^k \times \overline{\mathbb{R}}^k$, called *max-approximation* function, as follows. For $l \in \mathbb{R}^k$ and $\widehat{l} \in \overline{\mathbb{R}}^k$, $\left(\overline{\Lambda}\left(l, \widehat{l}\right)\right)_i = \begin{cases} \widehat{l}_i & \text{if } \widehat{l}_i > \inf \\ l_i & \text{if } \widehat{l}_i = -\inf \end{cases}$.

Lemma 4. *Both the following statements are true.*

1. *Let* $l, u \in \mathbb{R}^k$ *and* $\widehat{l}, \widehat{u} \in \overline{\mathbb{R}}^k$. *Then,* $\overline{\Lambda}\left(l, \widehat{l}\right) \leq l \bigvee \widehat{l}$ *and* $\widehat{\Lambda}\left(u, \widehat{u}\right) \geq u \bigwedge \widehat{u}$.
2. *For fixed* $\widehat{l}, \widehat{u} \in \overline{\mathbb{R}}^k$, *the functions* $\overline{\Lambda}\left(., \widehat{l}\right) : \mathbb{R}^k \to \mathbb{R}^k$ *and* $\widehat{\Lambda}\left(., \widehat{u}\right) : \mathbb{R}^k \to \mathbb{R}^k$ *are both affine functions.*

4 Computation of positive invariants

In this section, we first derive a sufficient condition for positive invariance of an augmented complex zonotope. Also, we state conditions for containment of an initial set

and satisfaction of polytopic safety constraints. Latter, we explain how compute the augmented complex zontope based on these conditions.
Earlier, we had computed the linear transformations and Minkowki sums of augmented complex zonotope and possible overapproximations of their intersection with subparalleotopic constraints. Accordingly, we can compute the overapproximation of the reachable set of an augmented complex zonotope as another augmented complex zonotope. Then, we utilize the partial order given in Definition 6 to deduce a sufficient condition for positive invariance, as follows. We consider a state set Γ given as, for a location $q \in Q$, $\Gamma_q = \mathrm{Re}\left(\mathcal{G}\left(V_q, c_q, s_q, \mathcal{K}_q^\dagger, l_q, u_q\right)\right)$. Let us consider that the additive input for an intralocation transition in any location $q \in Q$ is overapproximated as $U_q \subseteq \mathcal{G}\left(V_q^{in}, c_q^{in}, s_q^{in}, W_q^{in}, l_q^{in}, u_q^{in}\right)$. Similarly, for an edge $\sigma \in E$, let the additive input set be overapproximated as $\Omega_\sigma \subseteq \mathcal{G}\left(V_\sigma^{in}, c_\sigma^{in}, s_\sigma^{in}, W_\sigma^{in}, l_\sigma^{in}, u_\sigma^{in}\right)$. Furthermore, for any $q \in Q$, the safe set in the location is $\mathcal{S}_q = \mathcal{J}\left(T_q, d_q\right)$ and the initial set is $\mathcal{I}_q = \mathrm{Re}\left(\mathcal{G}\left(V_q^I, c_q^I, s_q^I, W_q^I, l_q^I, u_q^I\right)\right)$.

Lemma 5 (Positive invariance). *The condition for positive invariance of the state set Γ is the following.*

1. *For any location $q \in Q$, the inclusion $R_q\left(\Gamma_q\right) \subseteq \Gamma_q$ holds if all of the below statements are collectively true.*

$$\begin{aligned} &\mathcal{K}_q^\dagger c_q = 0 \ \textit{i.e., primary offset is orthogonal to secondary template},\\ &\textit{there exist real vectors } c_q', s_q', l_q', u_q', l_q'', u_q'' \textit{ such that} \end{aligned} \tag{5}$$

(after intersection with staying conditions and affine transformation, variables are:)

$$\begin{aligned} c_q' &= \mathcal{A}_q c_q + c_q^{in}, \ \ s_q' = \begin{bmatrix} s_q \\ s_q^{in} \end{bmatrix} \\ l_q' &= \begin{bmatrix} \overline{\Lambda}\left(l_q, \gamma_q^-\right) \\ l_q^{in} \end{bmatrix}, \ \ u' = \begin{bmatrix} \widehat{\Lambda}\left(u_q, \gamma_q^+\right)) \\ u_q^{in} \end{bmatrix} \end{aligned} \tag{6}$$

(overapproximation after affine transformation:)

$$\mathcal{G}\left(\begin{bmatrix} \mathcal{A}_q V_q & V_q^{in} \end{bmatrix}, c_q', s_q', \begin{bmatrix} \mathcal{A}_q \mathcal{K}_q^\dagger & W_q^{in} \end{bmatrix}, l_q', u_q'\right) \sqsubseteq \mathcal{G}\left(V_q, c_q, s_q, \mathcal{K}_q^\dagger, l_q'', u_q''\right) \tag{7}$$

(post-transition inclusion after intersection with staying conditions:)

$$\overline{\Lambda}\left(l_q'', \gamma_q^-\right) \geq l_q \textit{ and } \widehat{\Lambda}\left(u_q'', \gamma_q^+\right) \leq u_q. \tag{8}$$

2. *For any edge $\sigma \in E$, the inclusion $R_\sigma\left(\Gamma_{\sigma_1}\right) \subseteq \Gamma_{\sigma_2}$ holds if all of the below statements are collectively true.*

$$\begin{aligned} &\mathcal{K}_{\sigma_1}^\dagger c_{\sigma_1} = 0 \ \textit{i.e., primary offset is orthogonal to secondary template},\\ &\textit{there exist real vectors } c_{\sigma_2}', s_{\sigma_2}', l_{\sigma_2}', u_{\sigma_2}', l_{\sigma_2}'', u_{\sigma_2}'' \ \textit{ such that} \end{aligned} \tag{9}$$

(affine transformation after intersection with staying conditions and guards:)

$$c_\sigma' = \Theta_\sigma c_{\sigma_1} + c_\sigma^{in}, \ \ s_\sigma' = \begin{bmatrix} s_{\sigma_1} \\ s_\sigma^{in} \end{bmatrix} \tag{10}$$

$$l'_\sigma = \begin{bmatrix} \overline{\Lambda}\left(l_{\sigma_1}, \gamma^-_{\sigma_1} \bigvee \sigma^-\right) \\ l^{in}_\sigma \end{bmatrix}, \;\; u' = \begin{bmatrix} \widehat{\Lambda}\left(u_{\sigma_1}, \gamma^+_{\sigma_1} \bigwedge \sigma^+\right) \\ u^{in}_\sigma \end{bmatrix} \tag{11}$$

(overapproximation after affine transformation:)

$$\mathcal{G}\left(\left[\Theta_\sigma V_{\sigma_1} \;\; V^{in}_\sigma\right], c'_\sigma, s'_\sigma, \left[\Theta_\sigma \mathcal{K}^\dagger_{\sigma_1} \;\; W^{in}_\sigma\right], l'_\sigma, u'_\sigma\right) \sqsubseteq \mathcal{G}\left(V_{\sigma_2}, c_{\sigma_2}, s_{\sigma_2}, \mathcal{K}^\dagger_{\sigma_2}, l''_\sigma, u''_\sigma\right) \tag{12}$$

(post-transition intersection with staying conditions and inclusion)

$$\overline{\Lambda}\left(l''_\sigma, \gamma^-_{\sigma_2}\right) \geq l_{\sigma_2} \text{ and } \widehat{\Lambda}\left(u'_\sigma, \gamma^+_{\sigma_2}\right) \leq u_{\sigma_2}. \tag{13}$$

Next, we state a sufficient condition for an augmented complex zonotopic state set to contain an initial set overapproximated by an augmented complex zonotope. This is given by the inclusion relation between augmented complex zonotopes from Lemma 3.

Lemma 6. *For a location $q \in Q$, $\mathcal{I}_q \subseteq \Gamma_q$ if,*

$$\mathcal{G}\left(V^I_q, c^I_q, s^I_q, W^I_q, l^I_q, u^I_q\right) \sqsubseteq \mathcal{G}\left(V_q, c_q, s_q, \mathcal{K}^\dagger_q, l_q, u_q\right). \tag{14}$$

For satisfaction of polytopic safety constraints by an augmented complex zonotope, the following lemma gives a sufficient condition, which is just the reformulation of 4 in the below context.

Lemma 7. *For any location $q \in Q$, $\Gamma_q \subseteq \mathcal{S}_q$ if,*

$$T_q\left(c_q + \mathcal{K}^\dagger_q\left(\frac{u_q + l_q}{2}\right)\right) + \left|T\left[V_q, \; \mathcal{K}^\dagger_q\right]\right| \begin{bmatrix} s \\ \frac{u_q - l_q}{2} \end{bmatrix} \leq d_q. \tag{15}$$

By simply collecting all the results of this section for computing a safe positive invariant, we state the following theorem.

Theorem 2. *If $\forall q \in Q$ and $\forall \sigma \in E$, all of the Equations[5-15] are collectively true, then the state set Γ is a positive invariant, satisfies the given safety constraints and contains the given initial set*

Solving the conditions. Firstly, we note that the secondary template in a location is predefined as the pseudoinverse of the subparallelotopic template in the location, in accordance with the above results in this section. Then, we observe that for a fixed primary template in each location, the set of Equations[5-15] are equivalent to second order conic constraints on the primary offset, upper and lower interval bounds in each location and some additional varaibles. This can be inferred from the Proposition 1 and the fact that the min-approximation and max approximation functions we defined earlier are affine. So, we first fix the primary template in each location and solve the aforementioned constraints as a convex program. The choice of the primary template is explained below.

Choosing the primary template. We may collect all or some of the following vectors in the primary template.

1. Eigenvectors of the transformation matrices and their products, for the different transition maps. This is because the eigenvectors can possibly capture some of the stable directions of the dynamics.
2. The primary and secondary templates of the augmented complex zonotopes which overapproimate the additive disturbance input sets. Also, we can incorporate the products of the linear matrices of the transition maps with these templates. This is because the input set and its transformations are added in reachable set computation.
3. Orthogonal projections of the above vectors on the null space of the subparallelotopic template. This is because the proposed intersection in Lemma 1 is exact when the primary template belongs to the null space of the subparallelotopic template.
4. Adding any set of arbitrary vectors will only increase the chance of computing a desired invariant, but at a computational expense. This is because the scaling factors will be adjusted accordingly by the optimizer.

5 Experiments

We performed experiments on three benchmark examples from the literature and compared the results with that obtained by the tool SpaceEx [9]. On one example, we compared the computational time with the reported results of the MPT tool [17]. For convex optimization, we used CVX (version 2.1) with MOSEK solver (version 7.1) and Matlab (version: 8.5/R2015a) on a computer with 1.4 GHz Intel Core i5 processor and 4 GB 1600 MHz DDR3. The precision of the solver is set to the default precision of CVX.

Robot with a saturated controller. Our first example is a benchmark model of a self-balancing two wheeled robot called NXTway-GS1 by Yorihisa Yamamoto, presented in the ARCH workshop [11]. The consider the sampled data (discrete time) networked control system model consisting of a plant and a controller, presented in the paper. In our experiment, we decoupled some unbounded directions of the dynamics of the system from bounded directions by making an appropriate linear transformation of the coordinates. The transformation is such that the coordinates corresponding to the *body pitch angle* and controller inputs are among the bounded directions. We do not explain the transformation here because it is beyond the scope of this paper. After such transformation, the dynamics of the system is given as $\left[\mathbf{x}(t+1)\ \mathbf{y}(t+1)\right]^T = F_1\mathbf{x}(t) + F_2 sat\left(\mathbf{y}(t)\right) + F_3\mathbf{u}(t)$. where the matrices F_1, F_2 and F_3 are given above the Table 2, $\mathbf{x}(t) \in \mathbb{R}^8$ is the transformed state of the composite system, $\mathbf{y}(t) \in \mathbb{R}^2$ is the input sent by the controller, $\mathbf{u}(t) \in [-100, 100]^4$ is the bounded additive disturbance input and sat is the saturation function which limits the controller input received by the plant, as follows. For the saturated system, $sat\left(y_i\right) = max\left(-\delta d_p, min\left(y_i, \delta d_p\right)\right),\ \forall i \in \{1, 2\}$, where $\delta = 100$ and $d_p = 0.0807$. For the unsaturated system, $sat\left(y_i\right) = y_i\ \forall i \in \{1, 2\}$. The state space of the saturated system can be divided into 9 different regions such that the system exhibits different affine dynamics in different regions. Therefore, the saturated sampled data system can be seen as a discrete time affine hybrid system. On the other hand, the unsaturated system has just one affine dynamics and is not a hybrid system. We model the saturated system using one location and nine self edges, corresponding to the nine different affine dynamics in different regions, which are specified

by the guards on the edges. The unsaturated system is modelled with one location and no edges such that the only dynamics is part of the intralocation affine dynamics. The same discrete time models are specified in SpaceEx for comparison of performance.
Size of unsaturated model: 10 dimensional, 1 location, 0 edges.
Size of saturated model: 10 dimensional, 1 location and 9 edges.
The safety requirement is that the *body pitch angle* of the robot, which in our model is denoted by x_1, should be bounded within some value. In the benchmark, it was suggested that $x_1 \in \left[-\frac{\pi}{2}+\epsilon, \frac{\pi}{2}-\epsilon\right] : \epsilon > 0$ for the saturated system, while $x_1 \in \left[\frac{-\pi}{2.26}, \frac{\pi}{2.26}\right]$ for the unsaturated system. The initial set is the origin.
Experiment settings. The primary template for the hybrid system is chosen as the collection of the (complex) eigenvectors of linear matrices of all affine maps for the edge transitions, the orthonormal vectors to the guarding hyperplane normals and the projections of the eigenvectors on the subspace spanned by the orthonormal vectors. For the linear system, it consists of the eigenvectors of the linear map, the input set template and its multiplication by the linear matrix (related to affine map) and square of the linear matrix. Concerning the experiment using SpaceEx, we tested with the octagon template and a template with 400 uniformly sampled support vectors. For the hybrid system, we computed a single augmented complex zonotopic invariant satisfying both the upper and lower safety bounds. But for the linear system, we computed two different invariants, each of which satisfies the upper and lower bounds, respectively.
Results. For both the hybrid and the linear systems, we could verify smaller magnitudes for the bounds on the pitch angle than what is proposed in the benchmark [11]. But the SpaceEx tool could not find a finite bound for either of the above systems. The results are reported in the Tables 1 and 2.
Remarks. We note that although in theory, a linear system has a polytopic invariant, but the number of faces of such a polytope can be arbitrarily large for any fixed dimension. In our unsaturated model which is linear, some of the eigenvalues are complex and their magnitudes are close to one. Possibly, this is the reason SpaceEx could not find an invariant even with 400 support vectors. But, since in our approach we use the complex eigen-structure, we could find the desired invariant for the unsaturated (linear) model. Furthermore, we we also computed the invariant for the saturated (hybrid) model.

Perturbed double integrator Our second example is a perturbed double integrator system given in [17]. The closed loop system with a feedback control is piecewise affine, having four different affine dynamics in four different regions of space, as $\mathbf{x}(t+1) = M_i\mathbf{x}(t) + w,$ where

$$i = \begin{cases} 1, \text{ if } x_1 \geq 0 \text{ and } x_2 \geq 0 \\ 2, \text{ if } x_1 \leq 0 \text{ and } x_2 \leq 0 \\ 3, \text{ if } x_1 \leq 0 \text{ and } x_2 \geq 0 \\ 4, \text{ if } x_1 \geq 0 \text{ and } x_2 \leq 0 \end{cases}, \; M_1 = M_2 = \begin{bmatrix} 0.4103 & 0.0653 \\ -0.2949 & 0.5327 \end{bmatrix}, \; M_3 = M_4 = \begin{bmatrix} 0.4103 & -0.0653 \\ 0.2949 & 0.5327 \end{bmatrix}$$

The additive disturbance input w is bounded as $\|w\|_\infty \leq 0.2$.
We perform two different experiments on this system. In the first experiment, we try to verify the smallest possible magnitude of bounds on the two coordinates, denoted x_1 and x_2. We compare these bounds with that found by the SpaceEx tool. In the second experiment, we try to quickly compute a large invariant for the system under the safety constraints given in [17]. In the latter case, we maximize the sum of the scaling factors and differences of the upper and lower interval bounds of the augmented complex

UB: >1000, NT: Not terminating in more than 180s,
n/a: Not applicable/not available, ACZ: Augmented complex zonotope.

$$F_1 = \begin{bmatrix} 3.6929 & 0 & 0.7302 & 7.9715 & 14.5019 & -0.0072 & 0.0720 & -2.7354 \\ 3.6929 & 0 & 0.7302 & 7.9715 & 14.5019 & -0.0072 & 0.0720 & -2.7354 \\ 0.9562 & 0 & 0.0019 & -0.0021 & -0.0022 & -0.0000 & -0.0001 & -0.0002 \\ 0 & 0.6910 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.8833 & 0 & -0.1154 & -1.2943 & -2.3520 & 0.0012 & -0.0118 & 0.4427 \\ -0.4712 & 0 & -0.0812 & 0.1151 & -1.4845 & 0.0007 & -0.0071 & 0.2819 \\ -0.1560 & 0 & -0.0459 & -0.3173 & 0.3650 & 0.0003 & -0.0023 & 0.1162 \\ -0.7719 & 0 & -0.1248 & -1.4264 & -2.5901 & 0.9973 & -0.0131 & 0.4869 \\ -0.7544 & 0 & -0.1243 & -1.4204 & -2.5792 & 0.0013 & 0.9825 & 0.4796 \\ -0.1905 & 0 & -0.0148 & -0.2081 & -0.3751 & 0.0002 & 0.0033 & 1.0651 \end{bmatrix}$$

$$F_2 = \begin{bmatrix} 0.2543 & 0.2543 \\ 0.2543 & 0.2543 \\ -0.0001 & -0.0001 \\ 0 & 0 \\ -0.0413 & -0.0413 \\ 0.0219 & 0.0219 \\ 0.0102 & 0.0102 \\ 0.0431 & 0.0431 \\ 0.0428 & 0.0428 \\ 0.0065 & 0.0065 \end{bmatrix}, \; F_3 = 10^{-2} \times \begin{bmatrix} 0.0000 & 0 & -0.0330 & 2.0218 \\ 0 & 0 & -0.0330 & -2.0218 \\ 0 & 0 & -0 & 0 \\ -0 & 0 & 0 & 0.0109 \\ -0.0118 & 0 & 0.0172 & 0 \\ 0.0436 & 0 & 0.0003 & 0 \\ -0.0478 & 0 & 0.0034 & 0 \\ -13.3924 & 0 & 0.0062 & 0 \\ 0.0909 & 0 & 0.0061 & 0 \\ -0.0798 & 0 & 0.0017 & 0 \end{bmatrix}$$

Method		$\lvert\psi\rvert \leq$	Comp. time (s)
SpaceEx	octagon template	UB	NT
	400 support vectors	UB	NT
Suggested in [11]		1.39	n/a
ACZ invariant		1.29	4

Table 1: Unsaturated robot model: results

Method		$\lvert\psi\rvert \leq$	Comp. time (s)
SpaceEx	octagon template	UB	NT
	400 support vectors	UB	NT
Suggested in [11]		$1.571 - \epsilon$: $\epsilon > 0$	n/a
ACZ invariant		1.13	45

Table 2: Saturated robot model: results

Method		$\lvert x_1\rvert \leq$	$\lvert x_2\rvert \leq$	Comp. time (s)
SpaceEx	octagon template	0.38	0.43	1.7
	100 support vectors	0.38	0.43	23.6
ACZ invariant		0.38	0.36	5.1

Table 3: Small invariant computation: Perturbed double integrator

Method	Comp. time (s)
MPT tool [17]	107
ACZ	12

Table 4: Large invariant computation: Perturbed double integrator

Method		Slow switching				Fast switching			
		$-x_1 \leq$	$-x_4 \leq$	$-x_7 \leq$	Comp. time (s)	$-x_1 \leq$	$-x_4 \leq$	$-x_7 \leq$	Comp. time (s)
SpaceEx	octagon template	28	27	10	NT	UB	UB	UB	NT
	100 support vectors	28	25	13	1.3	UB	UB	UB	NT
Real zonotope [13]		25	25	10	n/a	n/a	n/a	n/a	n/a
ACZ invariant		28	26	12	12	46	54	57	12.6

Table 5: Networked vehicle platoon: results and matrices

zonotopic invaraint. Furthermore, we decompose the given safety constraints as the intersection of four different sets of safety constraints. For each set of safety constraints, we compute a large augmented complex zonotopic invariant. Then the desired invariant is the intersection of four augmented complex zonotopic invariants. Although we may not find the largest possible (maximal) invariant by this approach, still the optimizer would find a large invariant. We draw comparison in terms of the computation time with the reported result for the MPT tool [17].
In our formalism, we model the system with 4 locations and 12 edges connecting all the locations. Appropriate staying conditions are specified in each location, reflecting the division of the state space into different regions where the dynamics is affine. The initial set is the origin. The same model is specified in SpaceEx.
Size of model: 2 dimensions, 4 locations and 12 edges.
Experiment settings. For the primary template, we collected the (complex) eigenvectors of all linear matrices of the affine maps and their binary products. For the SpaceEx tool, we experimented with two different templates, the octagon template and a template with 100 uniformly sampled support vectors.
Results. In the first experiment, we verified smalled bounds for x_2 than that of SpaceEx, while the bounds verified for x_1 were equal for both methods. In our second experiment on this example, the computation time for finding a large invariant by our method is significantly smaller than that of the reported result for the MPT tool. The results are summarized in the Tables 3 and 4.

Networked platoon of vehicles Our third example is a model of a networked cooperative platoon of vehicles, which is presented as a benchmark in the ARCH workshop [13]. The platoon consists of three vehicles M_1, M_2 and M_3 along with a leader board ahead. The movement of the vehicles is dependent on the communication between them. In the benchmark proposal, the continuous time dynamics of the vechicles is described as a hybrid system with two possible dynamics, related to the presence and absence of communication between the vechicles, respectively. Furthermore, there are time constraints on when the switching can happen. The continuous time dynamics can be described as

$$\dot{x} = A_{q(c)}x + Bu : \ q(c) \in 1, 2 \ \ \wedge \ \ \dot{q}(c) = 0 \ \ \wedge \ \ \dot{c} = 1$$
$$\exists c \in C : \ q(c^+) \neq q(c) \ \wedge \ c^+ = 0.$$

where x is the state of the system, $u \in [-9, 1]$ is the additive disturbance input, c is a clock, q is an index for the type of dynamics and C is a set of clock instants when a switching can happen. The system matrices are given in [13]. Any upper bounds on $-x_1$, $-x_4$, and $-x_7$ provide lower limits on the reference distances of M_1, M_2 and M_3 to their successor vehicles, beyond which the platoon is guaranteed avoid collision. Therefore, the verification challange is to find the smallest possible upper bounds on $-x_1$, $-x_4$, and $-x_7$. The benchmark then provides the experimental results for the case when the minimum dwell time is 20 seconds, i.e., $C = \{c > 20\}$ (also specified in the distributed SpaceEx implementation[1]). In our experiment, apart from the case of the minimum dwell time of 20s (slow switching), we also study a case of fast switching where C is the set of all non-negative integer times. We could specify discrete time

[1] http://cps-vo.org/node/15096

models that overapproximate the reachable sets of both these above models. We do not explain the discretization procedure here, because it is beyond the scope of this paper.
Size of slow switching model: 9 dimensions, 2 locations and 4 edges.
Size of fast switching (integer times) model: 9 dimensions, 2 locations, 2 edges.
Experiment settings. We chose the primary template as the collection of the (complex) eigenvectors of linear matrices of the affine maps in the the two locations and their binary products, the axis aligned box template and the templates used for overapproximating the input sets. For the SpaceEx tool, we experimented with two templates, octagon and hundred uniformly sampled support vectors.
Results. For the large minimum dwell time of $20s$, the discrete time SpaceEx implementation and also a method based on using real zonotopes [13] could verify slightly smaller bounds compared to our approach. But for the small minimum dwell time ($1s$) model, SpaceEx could not even find a finite set of bounds, whereas our approach could verify a finite set of bounds. These results are reported in the Table 5.

6 Conclusion

References

1. A. Adimoolam and T. Dang. Template complex zonotopes for stability and invariant computation. In *American Control Conference (ACC), 2017*. IEEE, 2017.
2. A. S. Adimoolam and T. Dang. Using complex zonotopes for stability verification. In *American Control Conference (ACC), 2016*, pages 4269–4274. IEEE, 2016.
3. S. Bensalem, M. Bozga, J.-C. Fernandez, L. Ghirvu, and Y. Lakhnech. A transformational approach for generating non-linear invariants. In *International Static Analysis Symposium*, pages 58–72. Springer, 2000.
4. O. Bouissou, E. Goubault, S. Putot, K. Tekkal, and F. Vedrine. Hybridfluctuat: A static analyzer of numerical programs within a continuous environment. In *International Conference on Computer Aided Verification*, pages 620–626. Springer, 2009.
5. M. A. Colón, S. Sankaranarayanan, and H. B. Sipma. Linear invariant generation using nonlinear constraint solving. In *International Conference on Computer Aided Verification*, pages 420–432. Springer, 2003.
6. P. Cousot and N. Halbwachs. Automatic discovery of linear restraints among variables of a program. In *Conference Record of the Fifth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 84–97, Tucson, Arizona, 1978. ACM Press, New York, NY.
7. T. Dang and T. M. Gawlitza. Template-based unbounded time verification of affine hybrid automata. In *Asian Symposium on Programming Languages and Systems*, pages 34–49. Springer, 2011.
8. D. Delmas, E. Goubault, S. Putot, J. Souyris, K. Tekkal, and F. Védrine. Towards an industrial use of fluctuat on safety-critical avionics software. In *International Workshop on Formal Methods for Industrial Critical Systems*, pages 53–69. Springer, 2009.
9. G. Frehse, C. Le Guernic, A. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, and O. Maler. Spaceex: Scalable verification of hybrid systems. In *Proc. 23rd International Conference on Computer Aided Verification (CAV)*, LNCS. Springer, 2011.

10. K. Ghorbal, E. Goubault, and S. Putot. The zonotope abstract domain taylor1+. In *Computer Aided Verification, 21st International Conference, CAV 2009, Grenoble, France, June 26 - July 2, 2009. Proceedings*, pages 627–633, 2009.
11. T. Heinz, J. Oehlerking, and M. Woehrle. Benchmark: Reachability on a model with holes. In *ARCH@ CPSWeek*, pages 31–36, 2014.
12. B. Jeannet and A. Miné. Apron: A library of numerical abstract domains for static analysis. In *Computer Aided Verification*, pages 661–667. Springer, 2009.
13. I. B. Makhlouf and S. Kowalewski. Networked cooperative platoon of vehicles for testing methods and verification tools. In *ARCH@ CPSWeek*, pages 37–42, 2014.
14. A. Miné. A new numerical abstract domain based on difference-bound matrices. In *Programs as Data Objects, Second Symposium, PADO 2001, Aarhus, Denmark, May 21-23, 2001, Proceedings*, pages 155–172, 2001.
15. A. Platzer and E. M. Clarke. Computing differential invariants of hybrid systems as fixedpoints. In *International Conference on Computer Aided Verification*, pages 176–189. Springer, 2008.
16. S. Prajna and A. Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *International Workshop on Hybrid Systems: Computation and Control*, pages 477–492. Springer, 2004.
17. S. Rakovic, P. Grieder, M. Kvasnica, D. Mayne, and M. Morari. Computation of invariant sets for piecewise affine discrete time systems subject to bounded disturbances. In *Decision and Control, 2004. CDC. 43rd IEEE Conference on*, volume 2, pages 1418–1423. IEEE, 2004.
18. E. Rodríguez-Carbonell and A. Tiwari. Generating polynomial invariants for hybrid systems. In *International Workshop on Hybrid Systems: Computation and Control*, pages 590–605. Springer, 2005.
19. S. Sankaranarayanan, T. Dang, and F. Ivancic. Symbolic model checking of hybrid systems using template polyhedra. In *TACAS*, volume 4963 of *Lecture Notes in Computer Science*, pages 188–202. Springer-Verlag, 2008.
20. S. Sankaranarayanan, H. B. Sipma, and Z. Manna. Constructing invariants for hybrid systems. In *International Workshop on Hybrid Systems: Computation and Control*, pages 539–554. Springer, 2004.
21. S. Sankaranarayanan, H. B. Sipma, and Z. Manna. Non-linear loop invariant generation using gröbner bases. *ACM SIGPLAN Notices*, 39(1):318–329, 2004.
22. A. Tiwari, H. Rueß, H. Saïdi, and N. Shankar. A technique for invariant generation. *Tools and Algorithms for the Construction and Analysis of Systems*, pages 113–127, 2001.

Appendix

Proofs in section