Augmented Complex Zonotopes for Computing Invariants of Affine Hybrid Systems

Arvind Adimoolam(✉) and Thao Dang

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

Abstract. Zonotopes are a useful set representation for bounded time reach set computation of affine hybrid systems because of their closure under Minkowski sum and matrix multiplication operations. For unbounded time reach set approximation of arbitrarily switched affine hybrid systems, template complex zonotopes and a corresponding invariant computation procedure were introduced, which utilized the possibly complex eigenstructure of the affine maps. But a major hurdle in extending the technique for computing invariants of more general affine hybrid systems, where switching is state dependent and controlled by linear constraints, is that the class of template complex zonotopes is not closed under intersection with linear constraints. In this paper, we use a more expressive set representation called augmented complex zonotopes, for which we propose an algebraic over-approximation of the intersection with linear constraints. This over-approximation is then used to derive a set of second order conic constraints for computing an augmented complex zonotopic positive invariant for discrete time affine hybrid systems with additive disturbance input and linear safety constraints. We demonstrate the efficiency of this approach by experimenting on some benchmark examples.

1 Introduction

In the design of embedded and cyber-physical systems, one of the most important requirements is safety, which can be roughly stated as that the system will never enter a bad state. Safety verification for such systems are known to be computationally challenging due to the complexity resulting from the interactions among heterogenous components, having mixed (continuous and discrete) dynamics. In this paper, we focus on the problem of finding invariants for hybrid systems, which are widely recognized as appropriate 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 verification of transition systems and program analysis (see for example [8,10,11,16,34] and

This research work is partially supported by ANR project MALTHY.

A. Abate and G. Geeraerts (Eds.): FORMATS 2017, LNCS 10419, pp. 97–115, 2017.
DOI: 10.1007/978-3-319-65765-3_6

the developed techniques have been extended to continuous and hybrid systems [9,12,26,30,31,33]. Barrier certificates [23] 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, and these reachability computation techniques have been developed for continuous and hybrid systems. Many such techniques are based on iterative approximation of the reachable state on a step-by-step basis, which can be thought of as a set-based extension of 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 verification (except when the over-approximation error accumulation is not too bad that the safety can be decided). In contrast, invariants and barrier certificates are based on conditions that are satisfied at all times. Although solving these conditions often involves fixed point computation, by exploiting the structure of the dynamics (such as eigenstructures of linear systems), one can derive meaningful conditions which can significantly reduce the number of iterations until convergence.

Zonotopes have the advantage that they accurately capture matrix multiplication and linear transformation operations, but they are used mainly for bounded time reachability computation. For approximating unbounded time reachable sets of arbitrarily switched affine hybrid systems based on positive invariants, template complex zonotopes were introduced in [1], which have the following useful property. Any template complex zonotope generated by the eigenvectors of a Schur stable linear transformation is positively invariant with respect to the transformation. Therefore, template complex zonotopes can exploit the possibly complex eigenstructure of the system dynamics for computing invariants, while real zonotopes can not. However, a formidable hurdle using them for invariant computation of more general affine hybrid systems, where switching is state-dependent and controlled by linear constraints, is that we have to handle the intersection of template complex zonotopes with the guard sets that trigger switching. 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 address this problem as follows. We use a slightly more general set representation, called *augmented complex zonotope*, based on which we propose an algebraic overapproximation of the intersection with a class of linear constraints, called sub-parallelotopic. Henceforth, we derive a numerically efficiently solvable sufficient condition for computing an augmented complex zonotopic invariant 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 subparallelotopic constraints that we consider are quite general and can be used in the specification of many practical affine hybrid systems. We corroborate our

approach by presenting the experimental results for three benchmark examples from the literature.

Related work. For hybrid systems verification, convex polyhedra [11,18], and their special classes such as octagons [22] and zonotopes [15,20] and tropical polyhedra [5] are the most commonly used set representations. During reachability 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 is to fix the face normal vectors or generators, which leads to template convex polyhedra [12,29]. Although our template complex zonotopes proposed in [1] do not belong to the class of convex polyhedra, they follow the same spirit of controlling the complexity using templates. Set representations defined by non-linear constraints include ellipsoids [19], polynomial inequalities [7] and equalities [25], quadratic templates and piecewise quadratic templates [3,27,28], which are used for computing non-linear invariants. A major problem of template based approaches finding good templates. In this regard, using template complex zonotopes and the augmented version introduced in this paper, we can exploit eigen-structures of linear dynamics which reflect the contraction or expansion of a set by the dynamics, and define good templates for efficient convergence to an invariant (see Proposition 4.3 of [2]).

The extension to complex zonotope [2] is very similar in spirit to quadratic zonotopes [4] and more generally polynomial zonotopes [6]. 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 in this paper of coupling additional linear constraints with complex zonotopes is inspired by the work on constrained zonotopes proposed in [14,32] for computing intersection with linear constraints. But while [14,32] compute the intersection or its overapproximation, algorithmically, we instead derive a simple algebraic expression to overapproximate the intersection. This algebraic expression is latter used to obtain second order conic (convex) constraints, for invariant computation in a single step of convex optimization.

Organization. The rest of the paper is organized as follows. Firstly, we explain some of the mathematical notation used in this paper. Then in Sect. 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 Sect. 3, we present the set representation of augmented complex zonotopes and discuss some important operations and relations, in particular intersection with sub-parallelotopic constraints, projection in any direction, linear transformation, Minkowski sum and inclusion checking. In Sect. 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 Sect. 5, we report some experimental results. The conclusion and future work are given in Sect. 6.

Notation. Some notations for which we consider explanation may be required is described below. We denote $\overline{\mathbb{R}} = \mathbb{R} \bigcup \{-\infty, \infty\}$. If S is a set of complex numbers, then $\mathrm{Re}(S)$ and $\mathrm{Im}(S)$ represent the real and imaginary projections of S, respectively. If z is a complex number, then $|z|$ denotes the absolute value of z. On the other hand, if X is a complex matrix (or vector), then $|X|$ denotes the matrix (or vector) 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 $\mathcal{D}(z)$. The conjugate transpose of a matrix $V \in \mathbb{M}_{m \times n}(\mathbb{C})$ is denoted $V^* = (\mathrm{Re}(V) - i\ \mathrm{Im}(V))^T$. If VV^* is invertible, then $V^\dagger = V^* (VV^*)^{-1}$, which is the pseudo-inverse of V. Given two vectors $l, u \in \mathbb{R}^k$ and any relation $\bowtie$ between numbers in $\overline{\mathbb{R}}$, we say $l \bowtie u$ if $l_i \bowtie u_i,\ \forall i \in \{1, ..., k\}$. The meet of the two vectors l and u 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, there is 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 $n \in \mathbb{Z}_{>0}$. For each location, a set of linear constraints called staying conditions constrain the continuous state of the system in the location. Also, there is an affine transition map with a (possibly) additive uncertain but bounded disturbance input set, which specifies the evolution of the continuous variables in the location. A set of labeled directed edges specify the discrete transitions, which result in a possible change of locations along with an affine reset of continuous variables, where the reset has a bounded additive uncertainty. Also, each edge transition can have a set of preconditions, called a guard, given by linear constraints.

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.

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 as a* sub-parallelotopic template. *Let $\widehat{u}, \widehat{l} \in \overline{\mathbb{R}}^k$ such that $\widehat{l} \leq \widehat{u}$. Then a sub-parallelotopic set is $\mathcal{P}\left(K, \widehat{l}, \widehat{u}\right) = \left\{x \in \mathbb{R}^n : \widehat{l} \leq Kx \leq \widehat{u}\right\}$.*

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. Sub-parallelotopic constraints are algebraically related to a generator representation. We can express $\mathcal{P}\left(K_{k\times n}, \widehat{l}, \widehat{u}\right) = \left\{c + K^{\dagger}\zeta : c \in \mathbb{R}^n, \zeta \in \mathbb{R}^k, Kc = 0, \widehat{l} \leq \zeta \leq \widehat{u}\right\}$. Here, the columns vectors in the pseudo-inverse $K^{\dagger}$ can be considered as generators. Therefore, it is possible to express the intersection of sub-parallelotope with a suitably aligned zonotope as a simple algebraic expression, as we will see latter.

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. 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, given as $\mathcal{P}\left(\mathcal{K}_q, \gamma_q^-, \gamma_q^+\right)$. A matrix A_q and a bounded set $U_q \subseteq \mathbb{R}^n$ correspond to the affine transformation 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 $\Omega_\sigma \subseteq \mathbb{R}^n$ correspond to the affine transition map along the edge.

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. Continuous transition.

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

2. Discrete transition.

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

Given a set of continuous states $S \in \mathbb{R}^n$ in a location, for computing the set of reachable continuous states in the next step of continuous or discrete transition, we define the following functions, respectively.

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

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

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

3 Augmented Complex Zonotopes

Before introducing augmented complex zonotope, we briefly review the related set representations used in this paper. First, 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 by $\mathcal{J}(T, d)$, 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 the halfspace polytopic representation is possible. However, in general, zonotopes do not admit efficient halfspace representations as polytopes. The reason is that a zonotope with m generators in an n-dimensional space has $\binom{m}{n-1}$ faces (bounding hyperplanes), if all combinations of any 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 continuous linear systems. Nevertheless, a major drawback of zonotopes is that their intersection with sets defined by linear constraints need not be zonotopes. Also, there is no unique smallest zonotope

that overapproximates such intersections. However, we observe that when the linear constraints constitute a sub-parallelotope with a template aligned with that of the zonotope, their intersection can be exactly computed. This is also the reason we considered the case of staying conditions and guards specified as sub-parallelotopes in this work. As a simple example, the intersection of $\mathcal{Z}\left(\begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}-1\\-1\end{bmatrix}, \begin{bmatrix}2\\2\end{bmatrix}\right)$ with $x_1 \leq 1 \wedge x_2 \geq 0.5$ gives $\mathcal{Z}\left(\begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}-1\\0.5\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}\right)$. The general case is described in the following lemma.

Lemma 1. *Let $K \in \mathbb{M}_{k\times n}(\mathbb{R})$ such that $k \leq n$ and $\left(KK^T\right)$ is non-singular. Then*

$$\mathcal{Z}\left(K^\dagger, l, u\right) \bigcap \mathcal{P}\left(K, \widehat{l}, \widehat{u}\right) = \mathcal{Z}\left(K^\dagger, l \bigvee \widehat{l}, u \bigwedge \widehat{u}\right)$$

A template complex zonotope introduced in [1] has complex valued vectors as generators, whose combining coefficients are complex and bounded in their absolute values. It has the useful property that when multiplied by a Schur stable matrix whose (possibly complex) eigenvectors are its generators, the transformed complex zonotope is contained inside the original complex zonotope. A formal statement of a similar property is given in Proposition 4.3 of [2]. Because of this property, template complex zonotopes can utilize the possibly complex eigenstructure while computing invariants.

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: $\mathcal{C}\left(V, c, s\right) = \{c + V\epsilon : \epsilon \in \mathbb{C}^m,\ |\epsilon_i| \leq s_i\ \forall i \in \{1, ..., m\}\}$.*

We note that unlike real zonotopes, template complex zonotopes can have non-polyhedral real projections because they describe Minkowski sums of ellipsoids and line segments. We now introduce an *augmented complex zonotope*, which is a 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 4 (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*

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

We first discuss the intersection operation of an augmented complex zonotope with sub-parallelotopic constraints, before discussing other operations. Note that due to the space limit, we do not include all the proofs but only those of the key results.

For deriving a formula for the intersection, we first prove some results on intersection among convex sets. Let us define the support of a vector v in a set $S \subset \mathbb{R}^n$ relative to a point $w \in \mathbb{R}^n$ as $\rho(v, w, S) = \max_{x \in S} v^T (x - w)$. The following lemma states a relationship between the support of vectors and inclusion between sets.

Lemma 2. *Let $S_1, S_2 \subseteq \mathbb{R}^n$ be two closed convex sets such that $S_1 \bigcap S_2 \neq \emptyset$. Let $w \in S_1 \bigcap S_2$. Then $S_1 \subseteq S_2$ iff $\forall v \in \mathbb{R}^n : \ \rho(v, w, S_1) \leq \rho(v, w, S_2)$.*

Let us say that two convex and closed sets S_1 and S_2 have non-empty intersection and w is a common point, i.e., inside the sets. According to the above lemma, saying that S_1 is contained inside S_2, is equivalent to saying that the maximum possible displacement in S_1 from w along the direction of any vector v is less than the maximum possible displacement in S_2 from w along the direction of the vector v.

Recall that an augmented complex zonotope is a Minkowski sum of a complex zonotope and a real zonotope, i.e., $\mathcal{C}(V, c, s) \oplus \mathcal{Z}(W, l, u)$. From Lemma 1, we see that the intersection of a sub-parallelotope $\mathcal{P}\left(K, \widehat{l}, \widehat{u}\right)$ with a zonotope $\mathcal{Z}(W, l, u)$ can be computed when $W = K^{\dagger}$. Motivated by this, we want to find a condition under which we can overapproximate the intersection $(\mathcal{C}(V, c, s) \oplus \mathcal{Z}(W, l, u)) \bigcap \mathcal{P}\left(K, \widehat{l}, \widehat{u}\right)$ by $\mathcal{C}(V, c, s) \oplus \left(\mathcal{Z}(W, l, u) \bigcap \mathcal{P}\left(K, \widehat{l}, \widehat{u}\right)\right)$, that is computing first the intersection (which can be done efficiently) and then the Minkowski sum. Indeed we can find the required condition for a more general case of any three closed convex sets S_1, S_2, S_3 (that is, find a condition under which $(S_1 \oplus S_2) \bigcap S_3$ can be overapproximated by $S_1 \oplus (S_2 \bigcap S_3)$) and apply this result to augmented complex zonotopes. We state this condition as follows.

Lemma 3. *Let $S_1 \subseteq \mathbb{C}^n$ and $S_2, S_3 \in \mathbb{R}^n$ be closed convex sets such that $S_2 \cap S_3 \neq \emptyset$ and $0 \in S_1$. Then $(S_1 \oplus S_2) \bigcap S_3 \subseteq S_1 \oplus (S_2 \cap S_3)$.*

Proof. Firstly, the imaginary parts of both sides of above inequality are equal to $\mathrm{Im}(S_1)$ because $\mathrm{Im}(S_2) = \mathrm{Im}(S_3) = 0$. So, we show the inclusion of real parts. Let $w \in S_2 \bigcap S_3$. Then, since $0 \in S_1$, so $w = w + 0 \in S_1 \oplus S_2 \implies w \in (\mathrm{Re}(S_1) \oplus S_2) \bigcap S_3$. So, based on Lemma 2, it sufficient to prove that for all $v \in \mathbb{R}^n$,

$$\rho\left(v, w, (\mathrm{Re}(S_1) \oplus S_2) \bigcap S_3\right) \leq \rho(v, w, \mathrm{Re}(S_1) \oplus (S_2 \cap S_3)).$$

Let us define $a = \rho(v, 0, \mathrm{Re}(S_1))$, $b = \rho(v, w, S_2)$ and $c = \rho(v, w, S_3)$. Since, $0 \in \mathrm{Re}(S_1)$, so $a = \max_{x \in \mathrm{Re}(S_1)} v^T x \geq v^T 0 = 0$, i.e., $a \geq 0$. Furthermore, $\rho(v, w, (\mathrm{Re}(S_1) \oplus S_2) \bigcap S_3) = \min(\rho(v, w, \mathrm{Re}(S_1) \oplus S_2), \rho(v, w, S_3))$. As $w = w + 0$, so the above equals $\min(\rho(v, 0, \mathrm{Re}(S_1)) + \rho(v, w, S_2), \rho(v, w, S_3)) =$

$\min(a+b, c)$. By a similar calculation, we can show $\rho(v, w, \mathrm{Re}(S_1) \oplus (S_2 \cap S_3)) = a + min(b, c)$. So, we need to prove that $\min(a+b, c) \leq a + min(b, c)$. Since $a \geq 0$, so $\min(a + b, c) \leq \min(a + b, a + c) = a + \min(b, c)$. □

Now we introduce the following *affine* functions which are used latter to express the overapproximation of the intersection between an augmented complex zonotope and a sub-parallelotope. A binary function $\widehat{\Lambda} : \mathbb{R}^k \times \overline{\mathbb{R}}^k$, called *min-approximation* function, is defined as follows: for $u \in \mathbb{R}^k$ and $\widehat{u} \in \overline{\mathbb{R}}^k$, $\left(\widehat{\Lambda}(u, \widehat{u})\right)_i = \begin{cases} \widehat{u}_i & \text{if } \widehat{u}_i < \infty \\ u_i & \text{if } \widehat{u}_i = \infty \end{cases}$. Similarly, another binary function $\overline{\Lambda} : \mathbb{R}^k \times \overline{\mathbb{R}}^k$, called *max-approximation* function, is defined as follows: for $l \in \mathbb{R}^k$ and $\widehat{l} \in \overline{\mathbb{R}}^k$, $\left(\overline{\Lambda}\left(l, \widehat{l}\right)\right)_i = \begin{cases} \widehat{l}_i & \text{if } \widehat{l}_i > \infty \\ l_i & \text{if } \widehat{l}_i = -\infty \end{cases}$. It is easy to see that the min-approximation and max-approximation functions are affine, because for any one coordinate, a respective function is either a constant function or equal to the first argument, i.e., identity function. The following theorem states that an overapproximation of the intersection of an augmented complex zonotope with a sub-parallelotope can be expressed using these affine approximation functions.

Theorem 1. *Given a sub-parallelotope* $\mathcal{P}\left(\mathcal{K}, \widehat{l}, \widehat{u}\right)$ *and an augmented complex zonotope* $\mathcal{G}\left(V, c, s, \mathcal{K}^\dagger, l, u\right)$ *such that* VV^* *is non-singular,* $\left|V^\dagger c\right| \leq s$, $l \leq \overline{\Lambda}\left(l, \widehat{l}\right) \leq \widehat{\Lambda}(u, \widehat{u}) \leq u$, *then* $\mathcal{G}\left(V, c, s, \mathcal{K}^\dagger, l, u\right) \bigcap \mathcal{P}\left(\mathcal{K}, \widehat{l}, \widehat{u}\right) \subseteq \mathcal{G}\left(V, c, s, \mathcal{K}^\dagger, \overline{\Lambda}\left(l, \widehat{l}\right), \widehat{\Lambda}(u, \widehat{u})\right)$.

Proof Sketch. Consider $S_1 = \mathcal{C}(V, c, s)$, $S_2 = \mathcal{Z}\left(\mathcal{K}^\dagger, l, u\right)$ and $S_3 = \mathcal{P}\left(\mathcal{K}, \widehat{l}, \widehat{u}\right)$. First, we check that $0 \in S_1$ and $S_2 \bigcap S_3 \neq \emptyset$, and then we subsitute S_1, S_2 and S_3 in Lemma 3. To compute the intersection between S_2 and S_3, we use Lemma 1. □

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. Given $\mathcal{G}_1 = \mathcal{G}(V, c, s, W, l, u)$ and $\mathcal{G}_2 = \mathcal{G}(V', c', s', W', l', u')$, we have $\mathcal{G}_1 \oplus \mathcal{G}_2 = \mathcal{G}\left([V\ V'], c + c', \begin{bmatrix} s \\ s' \end{bmatrix}, [W\ W'], \begin{bmatrix} l \\ l' \end{bmatrix}, \begin{bmatrix} u \\ u' \end{bmatrix}\right)$.
3. The limits of the projection of an augmented complex zonotope along any direction can be computed as follows. For $v \in \mathbb{R}^n$,

$$\max_{x \in \mathcal{G}(V,c,s,W,l,u)} v^T x = v^T \left(c + W\frac{l+u}{2}\right) + \left|v^T [V\ W]\right| \left(\begin{bmatrix} s \\ \frac{u-l}{2} \end{bmatrix}\right) \tag{3}$$

To derive (3), we multiply the linear constraints with the center of the augmented complex zonotope and add an error term proportional to a set of scaling factors.

The center is $\left(c + W\frac{l+u}{2}\right)$, while the scaling factors are $\begin{bmatrix} s \\ \frac{u-l}{2} \end{bmatrix}$. Based on (3), we derive the following Lemma relating the real projection of an augmented complex zonotope and a template complex zonotope.

Lemma 4. $\mathrm{Re}\left(\mathcal{G}\left(V, c, s, W, l, u\right)\right) = \mathrm{Re}\left(\mathcal{C}\left(\left[V\ W\right], c + W\left(\frac{u+l}{2}\right), \begin{bmatrix} s \\ \frac{u-l}{2} \end{bmatrix}\right)\right)$.

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. Therefore, we first review an inclusion relation between template complex zonotopes, which was earlier stated in [1].

Unlike usual zonotopes, template complex zonotopes can have non-polyhedral real projections. Checking the exact inclusion between two template complex zonotopes, in general, 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 5. *We define a relation "$\sqsubseteq$" between template complex zonotopes as $\mathcal{C}\left(V'_{n\times m'}, c', s'\right) \sqsubseteq \mathcal{C}\left(V_{n\times m}, c, s\right)$ if all of the below statements are collectively true.*

$$\exists X \in \mathbb{M}_{m\times m'}(\mathbb{C}) \text{ and } y \in \mathbb{C}^m \text{ s.t.}$$

$$VX = V'\mathcal{D}\left(s'\right), \quad Vy = c' - c, \text{ and } \max_{i=1}^{m}\left(|y_i| + \sum_{j=1}^{m'}|X_{ij}| - s_i\right) \leq 0 \tag{4}$$

Lemma 5 (Inclusion: template complex zonotopes). *The inclusion $\mathcal{C}\left(V', c', s'\right) \subseteq \mathcal{C}\left(V, c, s\right)$ holds if the relation $\mathcal{C}\left(V', c', s'\right) \sqsubseteq \mathcal{C}\left(V, c, s\right)$ 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. □

We extend the above inclusion relation to augmented complex zonotopes, based on Lemma 4 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 6 (Inclusion between 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 $\mathcal{G}\left(V', c', s', W', l', u'\right) \sqsubseteq \mathcal{G}\left(V, c, s, W, l, u\right)$ is true.*

For fixed V and V', we observe that (4) is equivalent to a set of convex constraints called second order conic constraints. Recall that a constraint of the

form $\|Ax\|_2 + v^T x + w \leq 0$ on an n-dimensional variable x, given $A \in \mathbb{M}_{n\times k}(\mathbb{R})$, $v \in \mathbb{R}^n$ and $w \in \mathbb{R}$, is a second order conic constraint (SOCC). We also note that linear inequalities and equalities can be expressed in the form of SOCC described above. There are many convex optimization tools that can efficiently solve SOCC up to a high numerical precision. Our aforementioned observation about (4) is extended to augmented complex zonotopes and formalized as below.

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

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 to 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 relation 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 $q \in Q$, $\Gamma_q = \mathrm{Re}\left(\mathcal{G}\left(V_q, c_q, s_q, \mathcal{K}_q^{\dagger}, l_q, u_q\right)\right)$ such that $V_q V_q^*$ is invertible. 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 $\mathcal{S}_q = \mathcal{J}(T_q, d_q)$ 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 7 (Positive invariance). *For all locations $q \in Q$ and all edges $\sigma \in E$, the inclusions $R_q(\Gamma_q) \subseteq \Gamma_q$ and $R_\sigma(\Gamma_{\sigma_1}) \subseteq \Gamma_{\sigma_2}$ holds if $\forall q \in Q$ and $\forall \sigma \in E$, all of the below statements are collectively true.*

/ intersection with staying conditions and one continuous transition */*

$$\left|V_q^{\dagger} c_q\right| \leq s_q,\ l_q \leq \overline{\Lambda}\left(l_q, \gamma_q^-\right) \leq \widehat{\Lambda}\left(u_q, \gamma_q^+\right)\right) \leq u_q \tag{5}$$

there exist real vectors $c_q', s_q', l_q', u_q', l_q'', u_q''$ such that

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

/ inclusion condition */*

$$\begin{aligned}&\mathcal{G}\left(\left[\mathcal{A}_q V_q \quad V_q^{in}\right], c_q', s_q', \left[\mathcal{A}_q \mathcal{K}_q^{\dagger} \quad W_q^{in}\right], l_q', u_q'\right) \sqsubseteq \mathcal{G}\left(V_q, c_q, s_q, \mathcal{K}_q^{\dagger}, l_q'', u_q''\right)\\ &l_q'' \leq \overline{\Lambda}\left(l_q'', \gamma_q^-\right) \leq \widehat{\Lambda}\left(u_q'', \gamma_q^+\right) \leq u_q'', \quad \overline{\Lambda}\left(l_q'', \gamma_q^-\right) \geq l_q \text{ and } \widehat{\Lambda}\left(u_q'', \gamma_q^+\right) \leq u_q.\end{aligned} \tag{7}$$

/ intersection with staying and guard condition of current location and one discrete transition*/*

$$\begin{aligned}&\text{there exist real vectors } c_{\sigma_2}', s_{\sigma_2}', l_{\sigma_2}', u_{\sigma_2}', l_{\sigma_2}'', u_{\sigma_2}'' \text{ such that}\\ &c_\sigma' = \Theta_\sigma c_{\sigma_1} + c_\sigma^{in}, \quad s_\sigma' = \begin{bmatrix} s_{\sigma_1} \\ s_\sigma^{in} \end{bmatrix}, \quad l_{\sigma_1} \leq \overline{\Lambda}\left(l_{\sigma_1}, \gamma_{\sigma_1}^-\right) \leq \widehat{\Lambda}\left(u_{\sigma_1}, \gamma_{\sigma_1}^+\right) \leq u_{\sigma_1}\end{aligned} \tag{8}$$

$$l_\sigma' = \begin{bmatrix} \overline{\Lambda}\left(l_{\sigma_1}, \gamma_{\sigma_1}^- \bigvee \sigma^-\right) \\ l_\sigma^{in} \end{bmatrix}, \quad u_\sigma' = \begin{bmatrix} \widehat{\Lambda}\left(u_{\sigma_1}, \gamma_{\sigma_1}^+ \bigwedge \sigma^+\right) \\ u_\sigma^{in} \end{bmatrix} \tag{9}$$

/ intersection with staying condition of target location and inclusion condition */*

$$\begin{aligned}&\mathcal{G}\left(\left[\Theta_\sigma V_{\sigma_1} \quad V_\sigma^{in}\right], c_\sigma', s_\sigma', \left[\Theta_\sigma \mathcal{K}_{\sigma_1}^{\dagger} \quad W_\sigma^{in}\right], l_\sigma', u_\sigma'\right) \sqsubseteq \mathcal{G}\left(V_{\sigma_2}, c_{\sigma_2}, s_{\sigma_2}, \mathcal{K}_{\sigma_2}^{\dagger}, l_\sigma'', u_\sigma''\right)\\ &l_\sigma'' \leq \overline{\Lambda}\left(l_\sigma'', \gamma_{\sigma_2}^-\right) \leq \widehat{\Lambda}\left(u_\sigma'', \gamma_{\sigma_2}^+\right) \leq u_\sigma''\\ &\overline{\Lambda}\left(l_\sigma'', \gamma_{\sigma_2}^-\right) \geq l_{\sigma_2} \text{ and } \widehat{\Lambda}\left(u_\sigma'', \gamma_{\sigma_2}^+\right) \leq u_{\sigma_2}.\end{aligned} \tag{10}$$

Next, for the augmented complex zonotopic state set to contain the initial set, we state the following sufficient condition based on the inclusion relation between augmented complex zonotopes from Lemma 6. For a location $q \in Q$, $\mathcal{I}_q \subseteq \Gamma_q$ if,

$$\mathcal{G}\left(V_q^I, c_q^I, s_q^I, W_q^I, l_q^I, u_q^I\right) \sqsubseteq \mathcal{G}\left(V_q, c_q, s_q, \mathcal{K}_q^{\dagger}, l_q, u_q\right). \tag{11}$$

For satisfaction of polytopic safety constraints, i.e., for a location $q \in Q$, $\Gamma_q \subseteq \mathcal{S}_q$, the following is a necessary and sufficient condition, which is a reformulation of (3).

$$T_q\left(c_q + \mathcal{K}_q^{\dagger}\left(\frac{u_q + l_q}{2}\right)\right) + \left|T\left[V_q, \ \mathcal{K}_q^{\dagger}\right]\right| \begin{bmatrix} s \\ \frac{u_q - l_q}{2} \end{bmatrix} \leq d_q. \tag{12}$$

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 Eqs. (5–12) 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. First 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 Eqs. (5–12) are equivalent to second order conic constraints on the primary offset, upper and

lower interval bounds in each location and some additional variables. This can be inferred from the Proposition 1 and the fact that the min-approximation and max approximation functions 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. Ensuring that the primary template has full rank, so that its pseudo-inverse as defined exists, 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 motivated by the observation that complex zonotopes generated by eigenvectors of a Schur stable matrix contract when multiplied by the matrix (see Proposition 4.3 of [2]). (2) The primary and secondary templates of the zonotopes which overapproximate the additive disturbance input sets and their products with the linear matrices of the transition maps. This is because the input set and its transformations are added in continuous step computation. (3) Orthogonal projections of the above vectors on the null space of the subparallelotopic template. This is because the proposed intersection in Theorem 1 is exact when the primary template belongs to the null space of the subparallelotopic template. (4) Adding any set of arbitrary vectors will 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 3 benchmark examples from the literature and compared the results with that obtained by the tool SpaceEx [13] which performs verification by step-by-step reachability computation. On one example, we compared the computational time with the reported results of the MPT tool [24]. 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 [17]. We consider the sampled data (discrete time) networked control system model 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.

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

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 [17]		1.39	n/a
ACZ invariant		1.29	4

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

Table 2. Saturated robot model: results

Method		$\lvert\psi\rvert \leq$	Comp. time (s)
SpaceEx	Octagon template	UB	NT
	400 support vectors	UB	NT
Suggested in [17]		$1.571 - \epsilon : \epsilon > 0$	n/a
ACZ invariant		1.13	45

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

Table 3. Small invariant computation: Perturbed double integrator

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 4. Large invariant computation: Perturbed double integrator

Method	Comp. time (s)
MPT tool [24]	107
ACZ	12

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 the continuous affine dynamics in the location. 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 com-

Table 5. Networked vehicle platoon: results and matrices

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 [21]		25	25	10	n/a	n/a	n/a	n/a	n/a
ACZ invariant		28	26	12	12	46	54	57	12.6

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

puted 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 [17]. 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.

Perturbed Double Integrator. Our second example is a perturbed double integrator system given in [24]. The closed loop system with a feedback control is piecewise affine, having four different affine dynamics in four different regions of space, as $\mathbf{x}(t+1) = M_i\mathbf{x}(t) + w$, $i \in \{1, 2, 3, 4\}$. 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 [24]. We draw comparison in terms of the computation time with the reported result for the MPT tool [24].

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 smaller 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 [21]. The platoon consists of three vehicles M_1, M_2 and M_3 along with a leader board ahead. In the benchmark proposal, the continuous time dynamics of the vehicles is described as a hybrid system with two possible dynamics, related to the presence and absence of communication between the vehicles, respectively. Furthermore, there are time constraints on when the switching can happen. The state of the system is a 9 dimensional vector x. 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 will not collide. Therefore, the verification challenge 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 s, 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 the possible switching times C is the set of all non-negative integers. We could specify discrete time models that overapproximate the reachable sets of both these above models.

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 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 20 s, the discrete time SpaceEx implementation and also a method based on using real zonotopes [21] could verify slightly smaller bounds compared to our approach. But for the small minimum dwell time (1 s) model, SpaceEx could not even find a finite set of bounds, whereas our approach could verify a finite set of bounds. The reason is that the system is more stable under slow switching as compared to fast switching. These results are reported in the Table 5.

6 Conclusion

We introduced augmented complex zonotopes as a more general set representation than template complex zonotopes, based on which we derived efficiently

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

solvable conditions for computing invariants, subject to linear safety constraints, for discrete time affine hybrid systems with linear guards and additive disturbance input. Like template complex zonotopes, augmented complex zonotopes have the advantage that we can meaningfully choose the templates for efficient fixpoint computation, based on the eigenstructure and other relevant aspects of the dynamics. But additionally, we overcame a drawback of template complex zonotopes in that we derived a simple algebraic expression for reasonable overapproximation of the intersection with a class of linear constraints. We use this algebraic expression to obtain of a set of second order conic constraints that can be efficiently solved to compute an invariant. In contrast to the step-by-step reachability computation approaches that iteratively accumulate overapproximation error, we instead compute an invariant in a single convex optimization step such that the optimizer inherently minimizes the overapproximation error. We demonstrated the efficiency of our approach on some benchmark examples.

As future work, we can investigate ways to minimize the overapproximation error in the intersection operation, such that the overapproximation can still be algebraically computed. In particular, the relation between the choice of the template and the over-approximation error in the intersection has to be analyzed. Also, we would like to extend this computational framework to continuous time hybrid systems.

References

1. Adimoolam, A., Dang, T.: Template complex zonotopes for stability and invariant computation. In: American Control Conference (ACC). IEEE (2017)
2. Adimoolam, A.S., Dang, T.: Using complex zonotopes for stability verification. In: American Control Conference (ACC), pp. 4269–4274. IEEE (2016)
3. Adjé, A.: Coupling policy iterations with piecewise quadratic lyapunov functions. In: Proceedings of the 20th International Conference on Hybrid Systems: Computation and Control (HSCC 2017), Pittsburgh, 18–20 April 2017, pp. 143–152 (2017)
4. Adjé, A., Garoche, P., Werey, A.: Quadratic zonotopes - an extension of zonotopes to quadratic arithmetics. In: Proceedings of the 13th Asian Symposium on Programming Languages and Systems (APLAS 2015), pp. 127–145 (2015)
5. Allamigeon, X., Gaubert, S., Goubault, É.: Inferring min and max invariants using max-plus polyhedra. In: Alpuente, M., Vidal, G. (eds.) SAS 2008. LNCS, vol. 5079, pp. 189–204. Springer, Heidelberg (2008). doi:10.1007/978-3-540-69166-2_13
6. Althoff, M.: Reachability analysis of nonlinear systems using conservative polynomialization and non-convex sets. In: Proceedings of the 16th International Conference on Hybrid Systems: Computation and Control (HSCC 2013), pp. 173–182 (2013)
7. Bagnara, R., Rodríguez-Carbonell, E., Zaffanella, E.: Generation of basic semi-algebraic invariants using convex polyhedra. In: Hankin, C., Siveroni, I. (eds.) SAS 2005. LNCS, vol. 3672, pp. 19–34. Springer, Heidelberg (2005). doi:10.1007/11547662_4
8. Bensalem, S., Lakhnech, Y.: Automatic generation of invariants. Form. Methods Syst. Des. **15**(1), 75–92 (1999)

9. Bouissou, O., Goubault, E., Putot, S., Tekkal, K., Vedrine, F.: HybridFluctuat: a static analyzer of numerical programs within a continuous environment. In: Bouajjani, A., Maler, O. (eds.) CAV 2009. LNCS, vol. 5643, pp. 620–626. Springer, Heidelberg (2009). doi:10.1007/978-3-642-02658-4_46
10. Colón, M.A., Sankaranarayanan, S., Sipma, H.B.: Linear invariant generation using non-linear constraint solving. In: Hunt, W.A., Somenzi, F. (eds.) CAV 2003. LNCS, vol. 2725, pp. 420–432. Springer, Heidelberg (2003). doi:10.1007/978-3-540-45069-6_39
11. Cousot, P., Halbwachs, N.: 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, Tucson, pp. 84–97 (1978)
12. Dang, T., Gawlitza, T.M.: Template-based unbounded time verification of affine hybrid automata. In: Yang, H. (ed.) APLAS 2011. LNCS, vol. 7078, pp. 34–49. Springer, Heidelberg (2011). doi:10.1007/978-3-642-25318-8_6
13. Frehse, G., et al.: SpaceEx: scalable verification of hybrid systems. In: Gopalakrishnan, G., Qadeer, S. (eds.) CAV 2011. LNCS, vol. 6806, pp. 379–395. Springer, Heidelberg (2011). doi:10.1007/978-3-642-22110-1_30
14. Ghorbal, K., Goubault, E., Putot, S.: The zonotope abstract domain Taylor1+. In: Bouajjani, A., Maler, O. (eds.) CAV 2009. LNCS, vol. 5643, pp. 627–633. Springer, Heidelberg (2009). doi:10.1007/978-3-642-02658-4_47
15. Girard, A.: Reachability of uncertain linear systems using zonotopes. In: Morari, M., Thiele, L. (eds.) HSCC 2005. LNCS, vol. 3414, pp. 291–305. Springer, Heidelberg (2005). doi:10.1007/978-3-540-31954-2_19
16. Goubault, E.: Static analysis by abstract interpretation of numerical programs and systems, and FLUCTUAT. In: Logozzo, F., Fähndrich, M. (eds.) SAS 2013. LNCS, vol. 7935, pp. 1–3. Springer, Heidelberg (2013). doi:10.1007/978-3-642-38856-9_1
17. Heinz, T., Oehlerking, J., Woehrle, M.: Benchmark: reachability on a model with holes. In: ARCH@ CPSWeek, pp. 31–36 (2014)
18. Jeannet, B., Miné, A.: Apron: a library of numerical abstract domains for static analysis. In: Bouajjani, A., Maler, O. (eds.) CAV 2009. LNCS, vol. 5643, pp. 661–667. Springer, Heidelberg (2009). doi:10.1007/978-3-642-02658-4_52
19. Kurzhanski, A., Varaiya, P.: Ellipsoidal techniques for reachability analysis: internal approximation. Syst. Control Lett. **41**(3), 201–211 (2000)
20. Maïga, M., Combastel, C., Ramdani, N., Travé-Massuyès, L.: Nonlinear hybrid reachability using set integration and zonotopic enclosures. In: European Control Conference (ECC 2014), Strasbourg, 24–27 June 2014, pp. 234–239 (2014)
21. Makhlouf, I.B., Kowalewski, S.: Networked cooperative platoon of vehicles for testing methods and verification tools. In: ARCH@ CPSWeek, pp. 37–42 (2014)
22. Miné, A.: The octagon abstract domain. High. Order Symb. Comput. **19**(1), 31–100 (2006)
23. Prajna, S., Jadbabaie, A.: Safety verification of hybrid systems using barrier certificates. In: Alur, R., Pappas, G.J. (eds.) HSCC 2004. LNCS, vol. 2993, pp. 477–492. Springer, Heidelberg (2004). doi:10.1007/978-3-540-24743-2_32
24. Rakovic, S., Grieder, P., Kvasnica, M., Mayne, D., Morari, M.: Computation of invariant sets for piecewise affine discrete time systems subject to bounded disturbances. In: 43rd IEEE Conference on Decision and Control (CDC 2004), vol. 2, pp. 1418–1423. IEEE (2004)
25. Rodríguez-Carbonell, E., Kapur, D.: Automatic generation of polynomial invariants of bounded degree using abstract interpretation. Sci. Comput. Program. **64**(1), 54–75 (2007)

26. Rodríguez-Carbonell, E., Tiwari, A.: Generating polynomial invariants for hybrid systems. In: Morari, M., Thiele, L. (eds.) HSCC 2005. LNCS, vol. 3414, pp. 590–605. Springer, Heidelberg (2005). doi:10.1007/978-3-540-31954-2_38
27. Roux, P., Garoche, P.-L.: Computing quadratic invariants with min- and max-policy iterations: a practical comparison. In: Jones, C., Pihlajasaari, P., Sun, J. (eds.) FM 2014. LNCS, vol. 8442, pp. 563–578. Springer, Cham (2014). doi:10.1007/978-3-319-06410-9_38
28. Roux, P., Jobredeaux, R., Garoche, P., Feron, E.: A generic ellipsoid abstract domain for linear time invariant systems. In: Hybrid Systems: Computation and Control (part of CPS Week 2012) (HSCC 2012), Beijing, 17–19 April 2012, pp. 105–114 (2012)
29. Sankaranarayanan, S., Dang, T., Ivančić, F.: Symbolic model checking of hybrid systems using template polyhedra. In: Ramakrishnan, C.R., Rehof, J. (eds.) TACAS 2008. LNCS, vol. 4963, pp. 188–202. Springer, Heidelberg (2008). doi:10.1007/978-3-540-78800-3_14
30. Sankaranarayanan, S., Sipma, H.B., Manna, Z.: Constructing invariants for hybrid systems. In: Alur, R., Pappas, G.J. (eds.) HSCC 2004. LNCS, vol. 2993, pp. 539–554. Springer, Heidelberg (2004). doi:10.1007/978-3-540-24743-2_36
31. Sassi, M.A.B., Girard, A., Sankaranarayanan, S.: Iterative computation of polyhedral invariants sets for polynomial dynamical systems. In: 53rd IEEE Conference on Decision and Control (CDC 2014), Los Angeles, 15–17 December 2014, pp. 6348–6353 (2014)
32. Scott, J.K., Raimondo, D.M., Marseglia, G.R., Braatz, R.D.: Constrained zonotopes: a new tool for set-based estimation and fault detection. Automatica **69**, 126–136 (2016)
33. Sogokon, A., Ghorbal, K., Jackson, P.B., Platzer, A.: A method for invariant generation for polynomial continuous systems. In: Jobstmann, B., Leino, K.R.M. (eds.) VMCAI 2016. LNCS, vol. 9583, pp. 268–288. Springer, Heidelberg (2016). doi:10.1007/978-3-662-49122-5_13
34. Tiwari, A., Rueß, H., Saïdi, H., Shankar, N.: A technique for invariant generation. In: Margaria, T., Yi, W. (eds.) TACAS 2001. LNCS, vol. 2031, pp. 113–127. Springer, Heidelberg (2001). doi:10.1007/3-540-45319-9_9