Safety Verification of Networked Control Systems by Complex Zonotopes

Arvind Adimoolam
Indian Institute of Technology Kanpur, Rajeev Motwani Building, Kalyanpur, Kanpur, India

Thao Dang
VERIMAG, CNRS/University Grenoble Alpes, Bâtiment IMAG, 700 Avenue Centrale, Grenoble, France

Abstract

Networked control systems (NCS) are widely used in real world applications because of their advantages, such as remote operability and reduced installation costs. However, they are prone to various inaccuracies in execution like delays, packet dropouts, inaccurate sensing and quantization errors. To ensure safety of NCS, their models have to be verified under the consideration of aforementioned uncertainties. In this paper, we tackle the problem of verifying safety of models of NCS under uncertain sampling time, inaccurate output measurement or estimation, and unknown disturbance input. Unbounded-time safety verification requires approximation of reachable sets by invariants, whose computation involves set operations. For uncertain linear dynamics, two important set operations for invariant computation are linear transformation and Minkowski sum operations. Zonotopes have the advantage that linear transformation and Minkowski sum operations can be efficiently approximated. However, they can not encode directions of convergence of trajectories along complex eigenvectors, which is closely related to encoding invariants. Therefore, we extend zonotopes to the complex valued domain by a representation called *complex zonotope*, which can capture contraction along complex eigenvectors for determining invariants. We prove a related mathematical result that in case of accurate feedback sampling, a complex zonotope will represent an invariant for a stable NCS. In addition, we propose an algorithm to verify the general case based on complex zonotopes, when there is uncertainty in sampling time and in input. We demonstrate the efficiency of our algorithm on benchmark examples and compare it with a state-of-the-art verification tool.

2012 ACM Subject Classification Computer systems organization → Reliability

Keywords and Phrases Safety Verification; Networked Control System; Reachability Analysis; Invariant; Complex Zonotope

Digital Object Identifier 10.4230/LITES.8.2.1

Received 2020-08-29 **Accepted** 2021-10-15 **Published** 2022-12-07

Editor Alessandro Abate, Uli Fahrenberg, and Martin Fränzle

Special Issue Special Issue on Distributed Hybrid Systems

1 Introduction

The computerized control of spatially distributed components through communication channels is called *networked control*. The emergence of fast and reliable communication networks has enabled efficient networked control of many applications in aerospace, automation, manufacturing and robotics [17, 26, 34, 37, 38]. Advantages of networked control systems (NCS) include reduced installation cost due to absence of wiring and remote operability. However, they are prone to inaccuracies in execution such as delays, packet dropouts and errors in sensing and quantization. To mitigate the risk of system failure, we need to verify the safety requirements of NCS in the presence of such inaccuracies. In this paper, we tackle the problem of verifying unbounded time safety of linear networked control systems with a uncertain sampling period for feedback input, inaccurate sensors for output estimation and disturbance input.

Safety verification involves proving that the set of reachable states of the system are contained within a specified safe set. However, exactly computing the set of reachable states of models containing linear differential equations with discontinuous switching between states or vector fields, called *affine hybrid systems*, is computationally intractable [13]. Instead, a common approach is to overapproximate this set of reachable states to prove safety. There has been a lot of research on overapproximating the set of reachable states of affine hybrid systems in both bounded and unbounded time [19, 32, 35]. But networked control systems have time triggered switching which can be handled accurately by these methods. The reason is explained below.

Challenge of safety verification of NCS

In an NCS, there is time triggered switching of states with uncertainty in the switching time (sampling time). The approach followed by most techniques [19, 32, 35] to overapproximate reachable sets of hybrid systems involves computing intersection between reachable sets and guard conditions by some set representation like polytopes [35], zonotopes [21], ellipsoids [10], or polynomial sub-level sets like barrier certificates [32]. In the case of NCS, the guard is on the time of switching, i.e., the clock variable. For very simple hybrid systems having constant vector fields, there is linear relationship between clock variables and other state variables. Then, we can expect to reliably overapproximate the intersection of guard on the clock variable and reachable states containing value of clock variable. But an NCS is more complex involving linear differential equations with time triggered switching. There is an exponential relationship between the clock variable and the reachable states in NCS. Such exponential relationship can not be captured using the well known set representations mentioned above. Instead, a more effective way is proposed in [8, 16, 18, 25, 31] to handle time triggered switching by dividing the switching time into very small sub-intervals and using matrix exponentials to map the reachable states in different sub-intervals. The above methods for stability verification of NCS do not consider additive input in the dynamics. However, our dynamics is more general where we consider consider additive disturbance input. The above methods [8, 16, 18, 25, 31] use ellipsoids and H-polytopes which do not efficiently handle additive input in high dimensions. Ellipsoids provide poor accuracy for approximating Minkowski sum with input sets, which is required in reachability analysis. Similarly, the complexity of H-polytopes exactly representing Minkowski sums blows up at least exponentially in the dimension of state space [28]. Therefore, we need better set representations to accurately overapproximate the reachable sets at various switching times.

Solution: Generalizing zonotope to complex zonotope

In this context, an effective set representation is a *zonotope* [20], described as a linear combination of real vectors called *generators*, whose combining coefficients are bounded in absolute value. Its advantage is that linear transformation and the Minkowski sum can be efficiently computed. However, we are required to overapproximate the unbounded time reachable set of NCS that typically involves computing *invariants*. Computing invariants by a set representation requires encoding the directions of convergence of reachable sets towards equilibrium. In NCS, some of the directions for convergence can be along the eigenvectors of the dynamics, which can be complex valued vectors (Theorem 7). But (simple) zonotopes, which are confined to the real valued domain, can fail to capture such complex valued directions of convergence of trajectories. Therefore, our goal is to extend them to the complex number domain to obtain a new set representation called *complex zonotope*. Complex zonotopes retain the merit of usual zonotopes that linear transformation and the Minkowski sum operations can be computed efficiently. Additionally, they can capture the contraction of reachable sets based on the complex eigenstructure, which is not possible using a real valued zonotope. We provide mathematical evidence (Theorem 7) to support the latter claim. Furthermore, their real projections are geometrically more expressive than usual zonotopes and can represent some non-polytopic sets.

Using complex zonotopes, we propose an algorithm to verify linear safety constraints of a linear NCS with uncertain sampling period, inaccurate output estimation and disturbance input. The algorithm is a semi-decision procedure which can either terminate when the system is verified to be safe or fail to terminate. In the latter case, the user can set a threshold number of iterations for termination to get a bounded time result. Using the algorithm, we successfully applied our algorithm to verify benchmark examples of NCS [23, 29] with high dimensions (≥ 12 dimensions (including state and controller input variables), while the simple zonotope based version of our algorithm and a state-of-the-art verification tool [19] both failed to verify them.

In summary, we make the following contributions in this paper.

1. We introduce the complex zonotope set representation, a geometrically more expressive representation than zonotope, to handle invariant computation in the presence of additive input and time triggered switching.
2. We propose a theoretical result (Theorem 7) about the existence of complex zonotopic invariants based on eigenvectors of the NCS dynamics.
3. We extend the previous algorithms for stability verification of NCS [8, 16, 18, 25, 31] without additive input to safety verification in the presence of additive input. We use complex zonotopes containing eigenvectors for computing invariants of NCS more effectively when there is additive input.
4. As a proof-of-concept, we compare the performance of our complex zonotope with a real zonotope containing concatenation of real and imaginary parts of the complex template. We compare the performance on high dimensional (>9 state space) benchmarks examples in literature. We show that while our complex zonotope is successful in verification, the real zonotope either fails to compute an invariant or computes one with very large bounds above the safety threshold. We also compare with another state-of-the-art tool [19], which also failed to verify the benchmarks.

This paper is an extended version of part of our work presented in the conferences [1–4] and the PhD thesis [5]. The extensions and modifications made in this paper are explained in Section 2.

Organization. In Section 2, we review previous research related to our work and draw some comparison. In Section 3, we formalize NCS with uncertainty in sampling time, inaccurate output estimation and unknown open loop input. We explain the relation between safety verification and invariant computation at sampling times for an NCS. In Section 4, we introduce the complex zonotope representation as a generalization of usual zonotopes to complex valued domain. We describe a result that shows how a complex zonotope can specify invariants based on eigenstructure. We discuss operations on complex zonotopes that are later used to verify safety properties. In Section 5, we describe the procedure for verification using complex zonotopes. The experiments on some benchmark examples and results are discussed in Section 6. We begin by describing in the following the mathematical notation used in this paper.

1.1 Notation

The set of real numbers is represented by $\mathbb{R}$, integers by $\mathbb{Z}$, and their positive subsets by $\mathbb{R}_{\geq 0}$ and $\mathbb{Z}_{\geq 0}$, respectively. The set of complex numbers is $\mathbb{C}$. Given a subset $\mathbb{S}$ of real or complex numbers we denote the set of n-dimensional vectors from $\mathbb{S}$ as $\mathbb{S}^n$ and $n \times m$ matrices from $\mathbb{S}$ as $\mathbb{S}^{n\times m}$. The i^{th} component of a vector x is x_i while the element of the i^{th} row and the j^{th} column of a matrix X is X_{ij}. The numbers of rows of matrix X and size of vector x are $\text{rows}\,(X)$ and $\text{rows}\,(x)$, respectively. The number of columns of X is $\text{cols}\,(X)$. Given any two real vectors x, y such that $\text{rows}\,(x) = \text{rows}\,(y)$, we say $x \leq y$, if $\forall i \in \{1, \ldots, \text{rows}\,(x)\}$, $x_i \leq y_i$. The diagonal matrix containing a vector x along its diagonal is denoted by $\mathcal{D}(x)$. The identity matrix of size $n \times n$ is denoted by $\mathcal{I}_n$ and a vector of ones of size n is denoted by $[1]_{n\times 1}$. The real part of a complex number x is $\mathrm{Re}(x)$ and the imaginary part is $\mathrm{Im}(x)$. The absolute value of a complex number x is $|x| = \sqrt{\mathrm{Re}(x)^2 + \mathrm{Im}(x)^2}$. The infinity norm of a complex vector x is $\|x\|_\infty = \max_{i=1}^{\mathrm{rows}(x)} |x_i|$. For a complex matrix X, $|X|$ is the matrix containing the absolute values of the elements of X, i.e., $|X|_{ij} = |X_{ij}|$. For any $a, b \in \mathbb{R} \bigcup \{\infty, -\infty\}$ we use the following notation for intervals.

$$(a,b) = \{x \in \mathbb{R} \mid a < x < b\}, \quad (a,b] = \{x \in \mathbb{R} \mid a < x \leq b\}$$
$$[a,b) = \{x \in \mathbb{R} \mid a \leq x < b\}, \quad [a,b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$$

Given two same dimensional subsets of complex vector space $U \in \mathbb{C}^n$ and $V \in \mathbb{C}^n$, we define their Minkowski sum as follows.

$$U \oplus V = \{u + v \mid u \in U,\ v \in V\}$$

Given a complex matrix $M \in \mathbb{C}^{n\times n}$ and a non-negative real matrix $\Upsilon \in \mathbb{R}_{\geq 0}^{n\times n}$, we define a neighborhood of M whose difference with M is less than Υ, as follows.

$$M \triangledown \Upsilon = \left\{ M + \widehat{M} \;\middle|\; \widehat{M} \in \mathbb{C}^{n\times n},\ \left|\widehat{M}\right| \leq \Upsilon \right\}.$$

2 Related work

This paper is a journal extension of part our work part on safety and stability verification using complex zonotope presented in the conferences [1–4] and a PhD thesis [5]. The present work adapts the algorithm used for stability verification [2, 4] and tackles the problem of safety verification of NCS. In this context, we provide a sufficient condition for checking inclusion of a set of complex zonotopes whose templates are in the neighborhood of a complex zonotope, inside another complex zonotope. This generalizes inclusion checking between two complex zonotopes from the conference papers [1, 5] to inclusion checking between a set of complex zonotopes and another complex zonotope. Our conference paper on safety verification [1] proposes an approximation of intersection of complex zonotope with linear constraints which can be coarse because complex zonotopes are not closed under intersection with linear constraints. If using this method for an NCS with uncertain sampling time, intersection of complex zonotopes with sampling time constraints can be inaccurately approximated. Instead, in this paper we make use of matrix exponential maps to compute an *invariant*.

A number of set representations have also been developed for verification of hybrid systems and also numerical programs. Linear relationships between state variables can be represented using polytopes [15] and their variants, such as template polyhedra [35], hypercubes [36], octagons [30], zonotopes [20] and tropical polyhedra [9]. Non-linear relationships between state variables can be encoded by ellipsoids [11, 27], polynomial templates [7, 33] and polynomial zonotopes [6, 12]. Similarly, a barrier certificate [32] can be used to separate the reachable set from an unsafe set using a sub-level set of a suitable function, such as a polynomial.

The efficiency of a set representation in verification depends on the efficiency of computing common operations used in reachability analysis. For a linear networked control system with additive uncertainty, linear transformation and the Minkowski sum are the main operations involved in the computation of the reachable sets. The zonotope representation [20] can be very efficient for *bounded time* reachability of a linear networked control system because the linear transformation and Minkowski sum over zonotopes can be computed efficiently. However, approximating *unbounded time* reachable sets typically requires computing invariants. Efficiently computing invariants requires encoding directions for convergence of state trajectories, which can depend on complex valued eigenvectors. But real valued zonotopes can not capture the convergence along complex valued eigenvectors. Therefore, we generalize zonotopes to complex zonotopes that can incorporate possibly complex eigenvectors among its generators in a way that the reachable set approximation can converge along the complex eigenvectors.

This generalization of zonotope to complex zonotope can express some non-polytopic sets in addition to polytopic zonotopes in the real domain, and hence more expressive. This generalization is similar in spirit to quadratic zonotope [6] or more generally polynomial zonotope [12] since both represent constraints on variables. However, while complex zonotope involves a linear combination of some ellipsoids and line segments, polynomial zonotope involves a non-linear combination of only line segments. Therefore, both represent very different classes of non-polyhedral sets. Moreover, we show in this paper that an infinite parametrized family of invariant complex zonotopes can be represented efficiently for any stable linear system using eigenvectors. However, there is no known guarantee of existence of invariant polynomial zonotopes, except trivially the equilibrium, for stable linear systems.

We remark that not many set representations can handle additive disturbance efficiently. Ellipsoids are not closed under the Minkowski sum [10], which can result in reduction of approximation accuracy in the presence of additive disturbance. The work of Allamigeon et. al [10] proposed an over-approximation of the Minkowski sum of ellipsoids based on the Löwner order, still the exact Minkowski sum can not be represented by an ellipsoid. Although polytopes are closed under Minkowski sum, there can be exponential blowup of complexity of the resulting half-space representation [28]. In contrast, zonotope and its extension to complex zonotope can exactly represent the Minkowski sum and its computation is also very efficient.

We draw inspirations from the algorithms for stability verification of sampled data systems which compute invariants [8, 16, 18, 25, 31] either as sub-level sets of Lyapunov functions or polytopes. In our work, we extend the use invariants to verify safety in addition to stability. Furthermore, our complex zonotope representation can efficiently handle additive disturbance due to efficient computation of the Minskowski sum. This is an advantage over sub-level sets of Lyapunov functions where the Minkowski sum can not be represented accurately, and also over polytopes whose representation is of exponential complexity [28].

3 Networked control systems

In a networked control system (NCS), a controller input is exchanged over a network between different components as information packets. The controller input is sampled at discrete time instants, while it remains constant between successive sampling times. But the sensors which estimate the output may be inaccurate and the sampling period can be uncertain, possibly due to packet dropouts. In this paper, we consider systems with linear dynamics, linear feedback input from the controller, uncertainty in sampling period and inaccurate output estimation modeled by additive error and additive disturbance input. This system can also be categorized as a hybrid system because of periodic reset of feedback input and constraints on its sampling period.

The system is modeled as follows. The state of the entire system at time $t \in [0, \infty)$ is $x_t \in \mathbb{R}^n$, the feedback input exchanged between components is $u_t \in \mathbb{R}^m$, disturbance input is $v_t \in V \subseteq \mathbb{R}^m$, output is $y_t \in \mathbb{R}^p$, additive error estimation is $w_t \in W \subseteq \mathbb{R}^p$, $\tau_{\min}$ is a lower bound on feedback sampling period, $\tau_{\max}$ is an upper bound on sampling time, the set of initial states is Ω and $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{m\times n}$, $C \in \mathbb{R}^{p\times n}$, $D \in \mathbb{R}^{p\times m}$, $F \in \mathbb{R}^{m\times p}$ are real matrices related to the system dynamics described below.

$$\begin{aligned}
&\exists\, (t_k)_{k=0}^{\infty}\,,\ \forall k \in \mathbb{Z}_{\geq 0} t_k \in \mathbb{R}_{\geq 0} \\
&\forall t \notin \bigcup_{k=0}^{\infty} \{t_k\}\,,\ \frac{\partial x_t}{\partial t} = Ax_t + Bu_t,\quad \frac{\partial u_t}{\partial t} = 0 && (1)\\
&\forall k \in \mathbb{Z}_{\geq 0},\quad y_{t_k} = Cx_{t_k} + Du_{t_k} + w_{t_k} && (2)\\
&u_{t_k} = Fy_{t_k} + v_{t_k} && (3)\\
&(t_{k+1} - t_k) \in [\tau_{\min}, \tau_{\max}],\ t_0 = 0,\ x_0 \in \Omega && (4)
\end{aligned}$$

We denote the combined vector of the state of the plant and controller input at any time t as $z_t = \left[x_t^T, u_t^T\right]^T$. We call a sequence of combined states at sampling times $(z_{t_k})_{k=0}^{\infty}$ as a sampling time trajectory which, by simple manipulation of the above equations, can be shown to be equivalently governed by the following dynamics.

$$\begin{aligned}
&z_{t_{k+1}} = R_{(t_{k+1}-t_k)} z_{t_k} + J_1 v_{t_{k+1}} + J_2 w_{t_{k+1}} \quad \text{where}\\
&\forall \tau \in [\tau_{\min}, \tau_{\max}],\ R_\tau = A_r \exp\left(A_c \tau\right),\\
&A_r = \begin{bmatrix} \mathcal{I}_n & 0 \\ FC & FD \end{bmatrix},\ A_c = \begin{bmatrix} A & B \\ 0 & 0 \end{bmatrix},\ J_1 = \begin{bmatrix} 0 \\ \mathcal{I}_m \end{bmatrix},\ J_2 = \begin{bmatrix} 0 \\ F \end{bmatrix} && (5)
\end{aligned}$$

▶ **Example 1** (Damped harmonic oscillator). We consider a damped harmonic oscillator where the feedback driving force is communicated over a network. The negative feedback driving force is $-x_1$ where x_1 is the position of the oscillator. In this case, we we have the following matrices for the dynamics.

$$A = \begin{bmatrix} 0 & 1 \\ 0 & -0.5 \end{bmatrix} \quad B = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad C = \begin{bmatrix} 1 & 0 \end{bmatrix} \quad D = 0 \quad F = -1$$

Then the equivalent matrices for the dynamics of combined states, i.e., A_c, A_r, J_1, J_2 and R_t for any $t \in [0, \infty)$ are the following.

$$A_c = \begin{bmatrix} 0 & 1 & 0 \\ 0 & -0.5 & 1 \\ 0 & 0 & 0 \end{bmatrix} \quad A_r = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix}$$

$$J_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \quad J_2 = \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix} \quad R_t = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix} \exp\left(\begin{bmatrix} 0 & t & 0 \\ 0 & -0.5t & t \\ 0 & 0 & 0 \end{bmatrix} \right)$$

3.1 Safety of NCS

Given a set of safe states $\mathcal{S} \subseteq \mathbb{R}^{n+m}$, we say that an NCS is safe if the state of plant, controller and feedback input of every trajectory at all times lies within $\mathcal{S}$. In other words, the set Γ of all reachable states defined as follows should lie within $\mathcal{S}$.

$$\Gamma = \left\{ \begin{bmatrix} x_\tau \\ u_\tau \end{bmatrix} \,\middle|\, \tau \in [0, \infty),\ (x_t, u_t)_{t \in [0,\infty)} \text{ satisfies (1)-(4)} \right\}$$

We shall show below that the safety of an NCS is guaranteed by the existence of an *invariant* set at sampling times that obeys certain conditions. We will later use this result to develop an algorithm for NCS safety verification.

▶ **Definition 2** (Sampling time invariant set)**.** A set Ψ of states is called a sampling time invariant if

$$\forall t \in [\tau_{\min}, \tau_{\max}],\ R_t \Psi \oplus J_1 V \oplus J_2 W \subseteq \Psi.$$

▶ **Theorem 3** (Relation between safety and sampling time invariant)**.** *For any $S \subseteq \mathbb{R}^{n+m}$, we have the reachable set Γ is included in $\mathcal{S}$, if there exists a sampling time invariant Ψ such that the following is true*

$$\forall \tau \in [0, \tau_{\max}],\ \exp\left(A_c \tau\right) \Psi \subseteq \mathcal{S} \tag{6}$$

$$\Omega \subseteq \Psi \tag{7}$$

Proof. Let us consider that at some sampling time t_k, a state $z_{t_k} \in \Psi$. Then at the next sampling time t_{k+1}, we get the following based on (5):

$$z_{t_{k+1}} \in R_{(t_{k+1}-t_k)} \Psi \oplus J_1 V \oplus J_2 W$$

We have $(t_{k+1} - t_k) \in [\tau_{\min}, \tau_{\max}]$ according to the dynamics of NCS. Therefore, according to the Definition 2 of sampling time invariant, we get $z_{t_{k+1}} \in \Psi$. This means that any state originating inside Ψ will remain inside Ψ at every sampling time. Since the initial set is contained in Ψ, *i.e.*, $\Omega \subseteq \Psi$, we get that for all possible trajectories of the system, the state remains within Ψ at the sampling time. Now, we have to prove that between any two sampling times, the state remains within the safe set.

Let $t = t_k + \tau$ be any time point where t_k is the latest sampling time before t, that is, $\tau \in [0, \tau_{\max}]$. Then the combined state reached at $t_k + \tau$ is given by

$$z_t = \exp\left(A_c \tau\right) z_{t_k}.$$

As we have shown that $z_{t_k} \in \Psi$, we get $z_t \in \exp\left(A_c \tau\right) \Psi$. It follows from (6), we get $z_t \in \mathcal{S}$, which proves the theorem. ◀

According to the above theorem, the safety of NCS can be verified by finding a sampling time invariant satisfying (6). The eigenstructure of the dynamics is closely related to sampling time invariants, which will be explained later in Theorem 7. Therefore, we introduce complex zonotope as a set representation in the next section, which enables us to use eigenvectors of the dynamics to find invariants. Complex zonotope also has other advantages, such as efficient computation of linear transformation and the Minkowski sum.

4 Complex zonotope

A simple zonotope is a set of points which are linear combinations of real vectors such that the combination coefficients are bounded in absolute values. Under this representation, the linear transformation and Minkowski sum can be exactly and quickly computed. This is useful for efficient bounded time reachability of a linear system as discussed in Girard *et al.* [20]. The mathematical definition of a simple zonotope or a real zonotope is as follows:

▶ **Definition 4** (Simple/Real zonotope)**.** Let P be a real valued matrix and $c \in \mathbb{R}^{\mathrm{rows}(P)}$ be a real vector. The following is a real zonotope centered at c.

$$\mathcal{Z}\left(P,\ c\right) = \left\{ P\zeta + c \,\middle|\, \zeta \in \mathbb{R}^{\mathrm{cols}(P)},\ \forall i \in \{1, \ldots, \mathrm{cols}\left(P\right)\}\ |\zeta_i| \leq 1 \right\}$$

We have discussed in the previous section that unbounded time safety verification of NCS is related to computing sampling time invariants. For a stable NCS with real eigenvectors, a set contracts along its eigenvectors. By incorporating such eigenvectors among the generators of a zonotope, we can find sampling time invariants. However, when the eigenvectors are complex valued, real zonotopes may not be able to represent the directions for convergence among its generators. Therefore, we extend real zonotopes to the complex number domain to represent complex valued eigenvectors among their generators to find positive invariants. We show in a later lemma that incorporating complex eigenvectors allows representing invariants for a stable linear system with possibly complex eigenvalues.

▶ **Definition 5** (Complex zonotope). Let $P \in \mathbb{C}^{\text{rows}(P) \times \text{cols}(P)}$ be a complex matrix, $c \in \mathbb{R}^{\text{rows}(P)}$ be a real vector and $s \in \mathbb{R}_{\geq 0}^{\text{cols}(P)}$ be a non-negative real vector. The following is a complex zonotope centered at c with template P and scale vector s.

$$\mathcal{Z}(P,\ c,\ s) = \left\{ P\zeta + c \;\middle|\; \zeta \in \mathbb{C}^{\text{cols}(P)},\ |\zeta| \leq s \right\}$$

While real zonotopes are a subclass of polytopes, real projections of complex zonotopes are more general and include non-polytopic sets in addition to polytopic zonotopes. Geometrically speaking, real projections of complex zonotopes are the Minkowski sum of some embedded ellipses and line segments.

▶ **Example 6.** Let us consider a complex zonotope $\mathcal{Z}(P,\ c,\ s)$ where

$$P = \begin{bmatrix} 1+2\iota & 1 & 2+\iota \\ 1-2\iota & 1 & 2-\iota \end{bmatrix}, \quad c = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad s = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

The real projection generated of $\mathcal{Z}\left(\begin{bmatrix} 1+2\iota \\ 1-2\iota \end{bmatrix},\ \begin{bmatrix} 0 \\ 0 \end{bmatrix},\ 1\right)$ is the ellipse $\left\{(x,y) \in \mathbb{R}^2 \;\middle|\; (x+y)^2 + \frac{(x-y)^2}{4} \leq 4\right\}$, real projection of $\mathcal{Z}\left(\begin{bmatrix} 2+\iota \\ 2-\iota \end{bmatrix},\ \begin{bmatrix} 0 \\ 0 \end{bmatrix},\ 1\right)$ is the ellipse $\left\{(x,y) \in \mathbb{R}^2 \;\middle|\; (x-y)^2 + \frac{(x+y)^2}{4} \leq 4\right\}$ and the real projection of $\mathcal{Z}\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix},\ \begin{bmatrix} 0 \\ 0 \end{bmatrix},\ 1\right)$ is the line segment $\left\{(x,y) \in \mathbb{R}^2 \mid -2 \leq x+y \leq 2\right\}$. So, the non-polytopic real projection of $\mathcal{Z}(P,\ c,\ s)$ in this example is the Minkowski sum of the two ellipses and one line segment as shown in Figure 1.

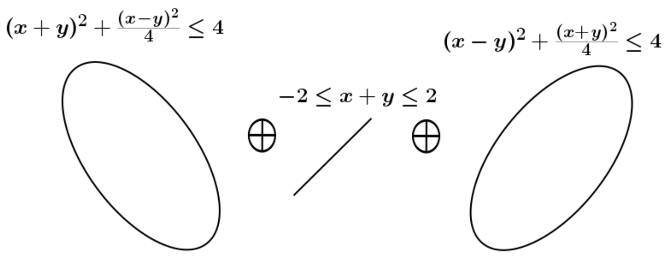

Figure 1 Complex zonotope as the Minkowski sum of two ellipsoids and a line segment

The following theorem states that when the sampling time period is certain, there is no additive disturbance input and the sampling time transformation matrix $R_{\tau_{\min}}$ is stable, we can find different sampling time invariant complex zonotopes by incorporating eigenvectors of the sampling time dynamics in its template and arbitrarily varying the scale factors.

▶ **Theorem 7** (Invariance based on eigenstructure). *Let us consider that $\tau_{\min} = \tau_{\max} = t$, $V = \{0\}$ and $W = \{0\}$. Let $E \in \mathbb{C}^{(n+m)\times(n+m)}$ contain the eigenvectors of R_t as its columns whose corresponding complex eigenvalues are $e \in \mathbb{C}^{(n+m)}$. If $0 < \|e\|_\infty \le 1$, then for any scale vector $s \in \mathbb{R}^n_{\ge 0}$, the complex zonotope $\mathcal{Z}(E,\ 0,\ s)$ is a sampling time invariant.*

Proof. Let $x \in \mathcal{Z}(E,\ 0,\ s)$. Based on the complex zonotope representation, there exists $\zeta \in \mathbb{C}^n, |\zeta| < s$ such that $x = E\zeta$. It then follows that

$$R_t x = R_t E \zeta = E\mathcal{D}(e)\zeta \tag{8}$$

Let $\alpha = \mathcal{D}(e)\zeta$. So $R_t x = E\alpha$ where we derive the following bound on th magnitude of α_i for any $i \in \{1, \ldots, n\}$.

$$|\alpha_i| = |e_i \zeta_i| = |e_i|\,|\zeta_i|$$

and since $\|e\|_\infty \le 1$, we have

$$|\alpha_i| \le |\zeta_i| \le s_i.$$

As $|\alpha| \le s$, we get $R_t x = E\alpha \in \mathcal{Z}(E,\ 0,\ s)$. Since this is true for all $x \in \mathcal{Z}(E,\ 0,\ s)$, we can establish that $R_t\mathcal{Z}(E,\ 0,\ s) \subseteq \mathcal{Z}(E,\ 0,\ s)$. ◀

▶ Remark (Advantage of complex zonotope over real zonotope). The above theorem is true for complex zonotopes but not for real zonotopes because real zonotopes can not have complex valued vectors as generators. Let us consider that the dynamics with constant sampling time has complex eigenstructure where the rank of eigenvectors is the total dimension $n + m$. The above theorem means that using complex zonotopes we can find a sampling time invariant set containing any initial set. However, using real zonotopes, we may not be able to find such a sampling time invariant set because real zonotopes capture contraction along complex eigenvectors. This is one main advantage of using complex zonotopes apart from being geometrically more expressive than real zonotopes. The below example illustrates how a complex zonotope sampling time invariant can be found by using the complex eigenvectors as generators. But a real zonotope invariant containing an initial set can not be found by using imaginary and real parts of eigenvectors and the coordinate directions as generators.

▶ **Example 8.** Let us consider the damped harmonic oscillator NCS in Example 1. Let us consider an initial set $\Omega = [-0.85, 0.85] \times [0, 0]$. Let us consider a complex matrix $P = \begin{bmatrix} -0.5774 & -0.5774 & -0.0051 \\ 0.1298 - 0.5626\iota & 0.1298 + 0.5626\iota & 0.1020 \\ 0.5774 & 0.5774 & -0.9948 \end{bmatrix}$. For $s = \begin{bmatrix} 29 \\ 0.8 \\ 0.8 \end{bmatrix}$, we get that $\mathcal{Z}\left(P,\ \begin{bmatrix} 0 \\ 0 \end{bmatrix},\ s\right)$ is a sampling time invariant of the NCS such that $\Omega \subseteq \mathcal{Z}(P,\ c,\ s)$. Now let us take the real matrix $G = \begin{bmatrix} \mathrm{Re}(P) & \mathrm{Im}(P) & \mathcal{I}_3 \end{bmatrix}$, which contains the real and imaginary parts of the complex matrix P as real generators and also the identity matrix. We used convex optimization (Algorithm 1) to search for a scaling factor h and center c such that the real zonotope $\mathcal{Z}(G,\ c,\ h)$ is a sampling time invariant containing the initial set. But our search failed to find it. Similarly, we tested with 5 uniformly randomly generated real valued templates, but all those real templates also could not be successful in finding an invariant. This illustrates that using complex zonotope containing eigenvectors as generators can let us find invariants in examples where real zonotopes may fail.

The result in Theorem 7 is only true when there is no uncertainty in sampling period. To handle a more general case where there is uncertainty in sampling period, we can incorporate eigenvectors of multiple matrices R_t for different values of $t \in [\tau_{\min}, \tau_{\max}]$. Then optimization can be used to find an appropriate scale factor that guarantees invariance, which we shall explain in Section 5.

As mentioned earlier, like real zonotopes, complex zonotopes are also closed under linear transformation and the Minkowski sum and they can be computed efficiently. This property is useful for efficiently representing sets of successor states of an NCS and is exploited in computing the operations used in our proposed NCS safety verification algorithm, namely Algorithm 1.

▶ **Lemma 9** (Linear transformation and the Minkowski sum). *Let us consider complex zonotopes $\mathcal{Z}(P,\ c,\ s) \subseteq \mathbb{C}^n$ and $\mathcal{Z}(Q,\ e,\ r) \subseteq \mathbb{C}^n$ and real matrices $A, B \in \mathbb{R}^{n\times n}$. Then the following is true:*

$$A\mathcal{Z}(P,\ c,\ s) \oplus B\mathcal{Z}(Q,\ e,\ r) = \mathcal{Z}\left(\begin{bmatrix}AP & BQ\end{bmatrix},\ Ac + Be,\ \begin{bmatrix}s\\ r\end{bmatrix}\right). \tag{9}$$

Proof. Let us consider $x \in \mathcal{Z}(P,\ c,\ s)$ and $y \in \mathcal{Z}(Q,\ e,\ r)$. Then there exist $\zeta, \alpha \in \mathbb{C}^n$ such that $|\zeta| \leq s$, $|\alpha| \leq r$, $x = P\zeta + c$ and $y = Q\alpha + e$. We derive the following:

$$\begin{aligned} &Ax + By = AP\zeta + Ac + BQ\alpha + Be \\ &\begin{bmatrix}AP & BQ\end{bmatrix}\begin{bmatrix}\zeta\\ \alpha\end{bmatrix} + (Ac + Be). \end{aligned}$$

We have $\left|\begin{bmatrix}\zeta\\ \alpha\end{bmatrix}\right| \leq \begin{bmatrix}s\\ r\end{bmatrix}$. Therefore, $Ax + By \in \mathcal{Z}\left(\begin{bmatrix}AP & BQ\end{bmatrix},\ Ac + Be,\ \begin{bmatrix}s\\ r\end{bmatrix}\right)$. Since this is true for all $x \in \mathcal{Z}(P,\ c,\ s)$ and $y \in \mathcal{Z}(Q,\ e,\ r)$, we obtain (9). ◀

In order to verify sampling time invariance of a complex zonotope given an interval of uncertainty, we need to check inclusion of a set of complex zonotopes (obtained by applying a sequence of transformations) inside the original complex zonotope, based on the Definition 2 of invariance. In this regard, we define a set of complex zonotopes whose templates lie in the neighborhood of a given template as follows. Let us consider a real matrix with positive entries $\Upsilon \in \mathbb{R}_{\geq 0}^{\mathrm{rows}(Q)\times \mathrm{cols}(Q)}$ where Q is a complex matrix and a real vector $\rho \in \mathbb{R}^{\mathrm{cols}(e)}$ where e is a real vector.

$$\mathcal{Z}(Q \bigtriangledown \Upsilon,\ e \bigtriangledown \rho,\ r) = \left\{\mathcal{Z}\left(Q + \widehat{Q},\ e + u,\ r\right)\ \Big|\ |Q| \leq \Upsilon,\ |u| \leq \rho\right\}$$

The following relation is a sufficient condition for checking the required inclusion which is proved later in Lemma 11.

▶ **Definition 10** (Relation for checking inclusion). Let P be a complex matrix such that $P^T P$ is a square invertible matrix. Let $\Upsilon > 0$ be a real matrix with only positive elements. We define the relation

$$\mathcal{Z}(Q \bigtriangledown \Upsilon,\ e \bigtriangledown \rho,\ r) \sqsubseteq \mathcal{Z}(P,\ c,\ s)$$

if all of the following conditions are verified:

$$\begin{aligned} &\exists X, \Delta \in \mathbb{C}^{\mathrm{cols}(P)\times \mathrm{cols}(Q)}, y \in \mathbb{C}^{\mathrm{cols}(P)}: \\ &PX = Q\mathcal{D}(r),\quad \Delta = \left|P^{\dagger}\right| \Upsilon \mathcal{D}(r),\quad (e - c) = Py,\quad \delta = \left|P^{\dagger}\right| \rho \end{aligned} \tag{10}$$

$$\forall i \in \{1, \ldots, \mathrm{rows}(X)\} \quad |y_i| + \delta_i + \sum_{j=1}^{\mathrm{cols}(X)} |X_{ij}| + \Delta_{ij} \leq s_i \tag{11}$$

▶ **Lemma 11** (Checking inclusion). *If $\mathcal{Z}(Q \bigtriangledown \Upsilon,\ e \bigtriangledown \rho,\ r) \sqsubseteq \mathcal{Z}(P,\ c,\ s)$ is true for $\Upsilon, \rho > 0$, then the subset inclusion $\mathcal{Z}(Q \bigtriangledown \Upsilon,\ e \bigtriangledown \rho,\ r) \subseteq \mathcal{Z}(P,\ c,\ s)$ is true.*

Proof. Let us assume that $\mathcal{Z}(Q \bigtriangledown \Upsilon,\ e \bigtriangledown \rho,\ r) \sqsubseteq \mathcal{Z}(P,\ c,\ s)$ is true. Hence, there exist matrices X, Δ and complex vectors y, ρ such that all the equations in (11) are true. Let us consider any $x \in \mathcal{Z}(Q \bigtriangledown \Upsilon,\ e,\ R)$. Based on the definition of a complex zonotope, there exists $\zeta \in \mathbb{C}^{\mathrm{cols}(P)}$ such that $|\zeta| \leq s$ and $x = \left(Q + \widehat{Q}\right)\zeta + e + u$, $\left|\widehat{Q}\right| \leq \Upsilon$ and $|u| \leq \rho$. We now have to show that $x \in \mathcal{Z}(P,\ c,\ s)$.

Let us consider a vector $\alpha \in \mathbb{C}^{\mathrm{cols}(\zeta)}$ such that for any $i \in \{1, \ldots, \mathrm{cols}(\zeta)\}$, the following is true:

$$\alpha_i = \zeta_i / r_i \ \text{ if } \ r_i > 0, \qquad\qquad \alpha_i = 0 \ \text{ if } \ r_i = 0 \tag{12}$$

Since $|\zeta| \leq r$, it follows from the above definition that $|\alpha| \leq 1$ and $\zeta = \mathcal{D}(r)\,\alpha$. Then we derive the following.

$$\begin{aligned} x &= \left(Q + \widehat{Q}\right)\zeta + e + u = \left(Q + \widehat{Q}\right)\mathcal{D}(r)\,\alpha + e + u \\ &= \left(Q + \widehat{Q}\right)\mathcal{D}(r)\,\alpha + (e - c) + c + u \end{aligned}$$

and from (10)

$$x = P\left(X\alpha + P^{\dagger}\widehat{Q}\mathcal{D}(r)\,\alpha + y + P^{\dagger}u\right) + c \tag{13}$$

We derive the following for any $i \in \{1, \ldots, \mathrm{rows}(X)\}$

$$\begin{aligned} &\left|X\alpha + P^{\dagger}\widehat{Q}\mathcal{D}(r)\,\alpha + y + P^{\dagger}u\right|_i \\ &\leq |y|_i + \left|P^{\dagger}\right||u| + \sum_{j=1}^{\mathrm{cols}(X)}\left(|X|_{ij} + \left(\left|P^{\dagger}\right|\left|\widehat{Q}\right|\mathcal{D}(r)\right)_{ij}\right)|\alpha|_j \\ &\leq |y|_i + \delta_i + \sum_{j=1}^{\mathrm{cols}(X)} |X|_{ij} + \Delta_{ij} \\ &\leq s_i. \end{aligned} \tag{14}$$

The above second inequality is true because $|\alpha| \leq 1$, $\left|\widehat{Q}\right| \leq \Upsilon$, $\Delta = \left|P^{\dagger}\right|\Upsilon\mathcal{D}(r)$, $|u| \leq \rho$ and $P^{\dagger}\rho = \delta$, and the last inequality is deduced from (11).

From (13) and (14), we get that $x \in \mathcal{Z}(P,\ c,\ s)$. As this is true for any $x \in \mathcal{Z}(Q,\ e,\ r)$, the inclusion $\mathcal{Z}(Q,\ e,\ r) \subseteq \mathcal{Z}(P,\ c,\ s)$ is true. ◀

We can algebraically compute bounds on the real projection of a complex zonotope along any direction, that is, the support function, as follows.

▶ **Lemma 12** (Computing support function)**.** *Let us consider a complex zonotope $\mathcal{Z}(P,\ c,\ s)$ and a vector $w \in \mathbb{R}^{\mathrm{cols}(c)}$. We have the following equality:*

$$\max_{x \in \mathcal{Z}(P,\ c,\ s)} \mathrm{Re}\left(w^T x\right) = w^T c + \left|w^T P\right| s \tag{15}$$

Proof. First we prove that

$$\max_{x \in \mathcal{Z}(P,\ c,\ s)} w^T x \leq w^T c + \left|w^T P\right| s \tag{16}$$

Let us consider $x \in \mathcal{Z}(P,\ c,\ s)$. So, there exists $\zeta \in \mathbb{C}^{\mathrm{cols}(P)}$ such that $|\zeta| \leq s$ and $x = P\zeta + c$. We derive the following:

$$\begin{aligned}\mathrm{Re}\left(w^T x\right) &= w^T c + \mathrm{Re}\left(w^T P \zeta\right) \\ &\leq w^T c + \left|w^T P\right| s\end{aligned} \tag{17}$$

The inequality in the above formula is deduced from the fact that $|\zeta| \leq s$. As the above is true for all $x \in \mathcal{Z}(P,\ c,\ s)$, it proves (16).

Next we prove the following:

$$\max_{x \in \mathcal{Z}(P,\ c,\ s)} w^T x \geq w^T c + \left|w^T P\right| s \tag{18}$$

Let us consider $x = P\zeta + c$ where $\zeta \in \mathbb{C}^{\mathrm{cols}(P)}$ is defined as follows.

$$\zeta_i = s_i \text{ if } \mathrm{Re}\left(w^T P_i\right) \geq 0, \qquad \zeta_i = -s_i \text{ otherwise} \tag{19}$$

Then we get the following:

$$\begin{aligned}\mathrm{Re}\left(w^T x\right) &= \mathrm{Re}\left(w^T P \zeta\right) + w^T c \\ &= \left|w^T P\right| s + w^T c\end{aligned}$$

The second equality in the above is obtained by using (19). This proves (18). From the inequalities (16) and (18), we get (15). ◀

The relation for checking inclusion ((10) and (11)) consists of a set of convex constraints on the variables X, Δ, s, r, e and c when the templates Q and P are fixed (constants). In fact, they constitute a class of convex constraints called *second order conic constraints* (SOCC) [14]. The SOCC constraints can be solved efficiently up to high numerical precision using convex optimization techniques and many solvers are available for the same [22].

5 Using complex zonotopes for verification

In this section, we describe an algorithm based on operations on complex zonotopes to verify safety of NCS. Our algorithm finds a complex zonotope which is a sampling time invariant and satisfies the other required condition (6) for safety. The algorithm has two parts.

1. We find a complex zonotope that is a sampling time invariant, *i.e.*, is invariant with respect to the transformation at all sampling times $t \in [\tau_{\min}, \tau_{\max}]$.
2. Next we verify that the the reachable set of the complex zonotope by continuous evolution, without reset, within the interval $[0, \tau_{\max}]$ remains within the safe set (6).

The detailed procedure is explained in Algorithm 1 and its correctness is proved in Theorem 17. A safe set is specified by linear constraints and an open input set, disturbance input set and initial set bounded by complex zonotopes, as follows.

$$\begin{aligned}&\mathcal{S} = \left\{x \in \mathbb{R}^{n+m} \mid Hx \leq d\right\}, \quad V \subseteq \mathcal{Z}\left(Q_V,\ c_V,\ s_V\right), \quad W \subseteq \mathcal{Z}\left(Q_W,\ c_W,\ s_W\right) \\ &\Omega \subseteq \mathcal{Z}\left(Q_{init},\ c_{init},\ s_{init}\right)\end{aligned}$$

Algorithm 1 Verifying safety of NCS.

$k \leftarrow 3$;
$P \leftarrow \begin{bmatrix} E_k & \mathcal{I}_{n+m} & R_{\tau_{\max}} & J_1 Q_V & J_2 Q_W \end{bmatrix}$;
Remove repeated columns and zero columns of P;
% Find sampling time invariant candidate complex zonotope:
$N \leftarrow 10$;
Feasible $\leftarrow$ *False*;
while *Feasible* $=$ *False* **do**
  Feasible $\leftarrow$ *True*;
  for $t \in \mathcal{T}_N$ **do**
    for $M \in \Theta\left(t, \mathcal{E}^t_{\frac{\tau_{\max}-\tau_{\min}}{N}}\right)$ **do**
      if *Feasible* $=$ *True* **then**
        Solve for s, c by convex optimization satisfying (24)–(25);
        if *(24)–(25) is feasible* **then**
          Feasible $\leftarrow$ *True*;
        else
          Feasible $\leftarrow$ *False*;
          $N \leftarrow 2 * N$;
        end
      end
    end
  end
end

% Verify Safety:
Verified $\leftarrow$ *False*;
while *Verified* $=$ *False* **do**
  Choose small $\epsilon > 0$;
  if *(26) is true* **then**
    Verified $\leftarrow$ *True*;
    Return: "NCS is safe"
  end
  else
    $\epsilon \leftarrow \epsilon/2$;
  end
end

5.1 Finding sampling time invariant

We first fix the template of a complex zonotope based on the eigenvectors of the dynamics and then the templates of the input sets. We can also add arbitrary vectors to the template to increase precision. Next we derive a set of convex constraints on center, scale factor and other auxiliary variables of a complex zonotope such that the complex zonotope is a sampling time invariant. We solve for the scale factor and center using convex optimization.

Let us choose a positive integer $k > 0$ and denote by E_k the matrix containing all independent unit eigenvectors of the matrices R_t for all $t \in \mathcal{T}_k$ where

$$\mathcal{T}_k = \left\{ t = \tau_{\min} + i\frac{\tau_{\max} - \tau_{\min}}{k} \;\middle|\; t \in [\tau_{\min}, \tau_{\max}] \right\}$$

The template P of the complex zonotope consists of these eigenvectors, the templates of inputs sets J_1Q_V, J_2Q_W, their transformations $R_{\tau_{\max}}J_1Q_V$, $R_{\tau_{\max}}J_2Q_W$.

$$P = \begin{bmatrix} E_k & \mathcal{I}_{n+m} & R_{\tau_{\max}} & J_1Q_V & J_2Q_W \end{bmatrix} \tag{20}$$

If P contains repeated columns or zero columns, they are removed.

▶ Remark (Choice of template). Firstly, we add the eigenvectors E_K of the transformation operators at various sampling times. This heuristic is based on Theorem 7 which says that incorporating eigenvectors in the complex zonotope is closely related to finding sampling time invariants. We also include the identity matrix inside the zonotope to capture bounds along the coordinate directions. Next, we get from Lemma 9 that the resulting complex zonotopes from applying the linear transformation R_t at time t is $R_t\mathcal{I}_{n+m}$ and R_tE_k. Since E_k contains eigenvectors of the dynamics at various sampling times, the directions of R_tE_k may not be very different from E_k. So, we do not include R_tE_k for any t. However, we include the other template $R_t\mathcal{I}_{n+m} = R_t$ at maximum sampling time $t_{\max}$ obtained by transforming the identity template. Next, by summing the additive disturbance and open input sets, we get the template $\begin{bmatrix} J_1Q_V & J_2Q_W \end{bmatrix}$ in a transformed complex zonotope after the switching at sampling time, by Lemma 9 . Therefore, this template is also concatenated to P_k. Furthermore, adding any arbitrary generator will only increase the accuracy because our optimization will adjust the scaling factors corresponding to the generators. So, we can increase the value of K to increase the accuracy of verification.

▶ **Example 13.** Let us consider the NCS in Example 1. We consider an lower bound $0.1s$ and upper bound $0.3s$ on the sampling time. We consider the safe set $\mathcal{S} = \left\{ z \in \mathbb{R}^3 \mid [100]z \le 1 \right\}$, initial set $\Omega = [0.85, 0.85] \times [0, 0] \times [0, 0]$, open input set $V = [-0.2, 0.2]$ and bounds on disturbance input set $W = [-0.2, 0.2]$. For $k = 3$, we compute E_k as the concatenation of eigenvectors of $R_{0.1} = A_r \exp(0.1A_c)$, $R_{0.2} = A_r \exp(0.2A_c)$ and $R_{0.3} = A_r \exp(0.3A_c)$ where A_r and A_c are given in Example 1.

Next we have to find the center and scale factor, for the given template P_k such that we get a sampling time invariant. Before we describe the algorithm for this, we derive the prerequisite mathematical results.

We can expand a transformation operator $R_{t+\delta}$ with $\delta > 0$ in a neighborhood of sampling time t using the Taylor expansion as follows.

$$R_{t+\delta} = A_r \exp(A_ct) \exp(A_c\delta) = R_t + R_tA_c\delta + R_tA_c\delta^2/2 + \Lambda_\delta \tag{21}$$
$$\text{where } |\Lambda_\delta| \le \mathcal{E}_\delta^t = |R_t| \left|\exp(A_ct)\right| |Ac|\delta^3/3.$$

We use the following lemma, which is proved in [24] to bound all matrices

$$\left\{ R_t + R_tA_c\delta + R_tA_c\delta^2/2 \mid \delta \le \epsilon \right\}$$

for any $\epsilon > 0$ by the convex hull of a finite set of matrices.

▶ **Lemma 14** ([25]). *Let $L_0, L_1, ..., L_r$ be a finite sequence of real matrices and $U_j(\delta) = \sum_{i=1}^{j} L_i\delta^i$. If $0 \le \delta < \epsilon$, then $U_r(\delta) \in \mathrm{Conv}(U_0(\epsilon), \ldots, U_r(\epsilon))$.*

Proof. This lemma is proved in [24]. ◀

Let us denote the set of finite matrices $\Theta(t,\epsilon) = \left\{\sum_{i=1}^{j} R_t A_c \epsilon^i \mid j = 0,1,2\right\}$. Then using Lemma 14, we have the following set inclusion:

$$\left\{R_t + R_t A_c \delta + R_t A_c \delta^2/2 \mid \delta \le \epsilon\right\} \subseteq \text{Conv}\left(\Theta(t,\epsilon)\right) \tag{22}$$

Therefore, using the expansion (21) and the above result (22), we get that for any $\epsilon > 0$ and $0 \le \delta \le \epsilon$,

$$R_{t+\delta} \in \text{Conv}\left(\left\{M \triangledown \mathcal{E}^t_\epsilon \mid M \in \Theta(t,\epsilon)\right\}\right)\ . \tag{23}$$

In order to verify sampling time invariance of $\mathcal{Z}(P,\ c,\ s)$, it is sufficient to divide the time interval $[\tau_{\min}, \tau_{\max}]$ into small intervals of a chosen size and verify invariance within each of the time intervals. This is explained in the following lemma.

▶ **Lemma 15.** *If there exists $N > 0$ such that $\forall t \in \mathcal{T}_N$, $\forall M \in \Theta\left(t, \frac{\tau_{\max}-\tau_{\min}}{N}\right)$ all of the following is true, then $\mathcal{Z}(P,\ c,\ s)$ is sampling time invariant.*

$$\exists \rho \in \mathbb{R}^{\text{cols}(c)}_{\ge 0} : \mathcal{E}^t_{\frac{\tau_{\max}-\tau_{\min}}{N}} |c| \le \rho \tag{24}$$

$$\mathcal{Z}\left(\begin{bmatrix} MP & J_1 & J_2 \end{bmatrix} \triangledown \begin{bmatrix} \mathcal{E}^t_{\frac{\tau_{\max}-\tau_{\min}}{N}} |P| & 0 & 0 \end{bmatrix},\ (Mc + J_1 c_v + J_2 c_w) \triangledown \rho,\ \begin{bmatrix} s \\ c_v \\ c_w \end{bmatrix}\right)$$
$$\sqsubseteq \mathcal{Z}(P,\ c,\ s) \tag{25}$$

Proof. Let us consider any $\tau \in [\tau_{\min}, \tau_{\max}]$. There exists $t \in \mathcal{T}_N$, $\delta \in \left[0, \frac{\tau_{\max}-\tau_{\min}}{N}\right]$ such that $\tau = t + \delta$. Then we derive the following.

$$R_\tau \mathcal{Z}(P,\ c,\ s) \oplus J_1 \mathcal{Z}(Q_V,\ c_V,\ s_V) \oplus J_2 \mathcal{Z}(Q_W,\ c_W,\ s_W)$$
$$= \mathcal{Z}\left(\begin{bmatrix} R_\tau P & J_1 Q_V & J_2 Q_W \end{bmatrix},\ R_\tau c + J_1 c_v + J_2 c_W,\ \begin{bmatrix} s & s_v & s_W \end{bmatrix}^T\right)$$
% *By* (23), $\exists M \in \Theta\left(t, \frac{\tau_{\max}-\tau_{\min}}{N}\right)$, $\exists \widehat{M} \in 0 \triangledown \mathcal{E}^t_{\frac{\tau_{\max}-\tau_{\min}}{N}} : R_\tau = M + \widehat{M}$
$$= \mathcal{Z}\left(\begin{bmatrix} MP & J_1 & J_2 \end{bmatrix} + \begin{bmatrix} \widehat{M} & 0 & 0 \end{bmatrix},\ Mc + \widehat{M}c + J_1 c_v + J_2 c_w,\ \begin{bmatrix} s & s_v & s_W \end{bmatrix}^T\right)$$
% *As* $\widehat{M} \in 0 \triangledown \mathcal{E}^t_{\frac{\tau_{\max}-\tau_{\min}}{N}}$ and $\mathcal{E}^t_{\frac{\tau_{\max}-\tau_{\min}}{N}} |c| \le \rho$ where $\mathcal{E}^t_{\frac{\tau_{\max}-\tau_{\min}}{N}} \ge 0$
$$\subseteq \mathcal{Z}\left(\begin{bmatrix} MP & J_1 & J_2 \end{bmatrix} \triangledown \begin{bmatrix} \mathcal{E}^t_{\frac{\tau_{\max}-\tau_{\min}}{N}} |P| & 0 & 0 \end{bmatrix},\ (Mc + J_1 c_v + J_2 c_w) \triangledown \rho,\ \begin{bmatrix} s \\ c_v \\ c_w \end{bmatrix}\right)$$
% *By (25) and Lemma 11 for inclusion checking*
$$\subseteq \mathcal{Z}(P,\ c,\ s)\,.$$

Since the above is true for any $\tau \in [\tau_{\min}, \tau_{\max}]$, we get that $\mathcal{Z}(P,\ c,\ s)$ is a sampling time invariant set. ◀

5.2 Safety verification

After finding a sampling time invariant containing the initial set, we have to verify that the condition (6) that the reachable set of $\mathcal{Z}(P,\ c,\ s)$ by continuous evolution within $[0, \tau_{\max}]$ is contained within the safe set. This can be verified by checking a sequence of linear inequalities as described in the following.

▶ **Lemma 16.** *For all $t \in [0, \tau_{\max}]$, we get $\exp(A_c t)\,\mathcal{Z}(P,\ c,\ s) \subseteq S$ if there exists $\epsilon > 0$ such that the following are true:*

$$\begin{aligned} &\forall k \in \mathbb{Z}_{\geq 0} :\ k \leq \frac{\tau_{\max}}{\epsilon},\ \forall i \in \{1, \dots, \text{rows}(H)\},\ \beta_i(P, c, s) \leq d \textit{ where} \\ &\beta_i(P, c, s) = |H_i \exp(A_c k\epsilon) P|\, s + H_i \exp(A_c k\epsilon)\, c \\ &\qquad + \|H_i\| \exp(\|A_c\|\,\epsilon)\, \|\exp(A_c k\epsilon)\|\, \epsilon\, (\|c\| + \|P\|\,\|s\|) \end{aligned} \tag{26}$$

Proof. Let us consider any $t \in [0, \tau_{\max}]$. There exists some $k \in \mathbb{Z}$, $t = k\epsilon + \rho$, $\rho \leq \epsilon$. We can write for $\rho \in [0, \epsilon]$,

$$\begin{aligned} &\exp(A_c\rho) = \sum_{i=0}^{n} \frac{A_c^i \rho^i}{i} = \mathcal{I}_{n+m} + A_c \rho M : \\ &M \in \mathbb{R}^{(n+m)\times(n+m)},\ \|M\| \leq \exp(\|A_c\|\,\epsilon) \end{aligned} \tag{27}$$

We derive the following:

$$\begin{aligned} H_i \exp(A_c t)\,\mathcal{Z}(P,\ c,\ s) &= H_i \mathcal{Z}(\exp(A_c t) P,\ \exp(A_c t) c,\ s) \\ &\quad \textit{\% By Lemma 12} \\ &\leq |H_i \exp(A_c t) P|\, s + H_i \exp(A_c t)\, c \\ &\quad \textit{\% By (27)} \\ &= |H_i \exp(A_c k\epsilon) P|\, s + H_i \exp(A_c k\epsilon)\, c + |H_i M P|\, s + Mc \\ &\quad \textit{\% Substituting the bound from (27)} \\ &\leq |H_i \exp(A_c k\epsilon) P|\, s + H_i \exp(A_c k\epsilon)\, c \\ &\quad + \|H_i\| \exp(\|A_c\|\,\epsilon)\, \|\exp(A_c k\epsilon)\|\, \|A_c\|\, \epsilon\, (\|c\| + \|P\|\,\|s\|) \leq d_i \end{aligned}$$

Therefore, $\exp(A_c t)\,\mathcal{Z}(P,\ c,\ s) \subseteq \{x \in \mathbb{R}^{n+m} \mid Hx \leq d\} = S$, which proves the lemma. ◀

The following theorem summarizes the overall sufficient condition for verifying safety based on complex zonotopes, which can be checked by the procedure described in Algorithm 1.

▶ **Theorem 17.** *We have $\Gamma \subseteq \mathcal{S}$ if there exist $c \in \mathbb{R}^n,\ s \in \mathbb{R}_{\geq 0}^{\text{cols}(P)}$, $\epsilon > 0$ and $N \in \mathbb{Z}_{\geq 0}$ such that all of the following conditions are true.*

1. *$\mathcal{Z}(Q_{init},\ c_{init},\ s_{init}) \sqsubseteq \mathcal{Z}(P,\ c,\ s)$.*
2. *(24)–(25) are true $\forall t \in \mathcal{T}_N,\ \forall M \in \Theta(t, \epsilon)$.*
3. *(26) is true.*

Proof. By ((24)-(25)) and Lemma 15, we prove that $\Psi = \mathcal{Z}(P,\ c,\ s)$ is a sampling time invariant. By the first condition $\mathcal{Z}(Q_{init},\ c_{init},\ s_{init}) \sqsubseteq \mathcal{Z}(P,\ c,\ s)$, we get that the initial set Ω is contained inside the sampling time invariant Ψ. By (26) and Lemma 16, we prove that for all $t \in [0, \tau_{\max}], \exp(A_c t)\,\mathcal{Z}(P,\ c,\ s) \subseteq \mathcal{S}$. Then based on Theorem 3, we get $\Gamma \subseteq \mathcal{S}$. ◀

Based on Theorem 17, we propose a semi-decision procedure in Algorithm 1 to verify safety. The algorithm is a semi-decision procedure because if it returns that the NCS is safe, then the NCS is indeed safe as proved in Theorem 17. However, the algorithm is not guaranteed to terminate. So, the user can choose to terminate the algorithm in any threshold number of iterations possibly with inconclusive result. In this context, we note NCS is a hybrid system and it is known that verification of reachability of very simple classes of hybrid systems is undecidable [13]. So, it is unlikely that we can not come up with a sure shot decision procedure to verify safety of NCS.

▶ **Example 18.** Let us the NCS in Example 13. We took $K = 3$ and ran our algorithm using the template matrix containing complex eigenvectors as shown in Equation 20, without any random matrix, i.e., $\Pi = 0$. Then we could verify that the x_1 bounds on the unbounded time reachable set is $|x_1| \leq 2.22$.

Comparison with real zonotope. Next, we concatenated the real and imaginary parts of P_k into a real matrix G where repeated column vectors were removed. We ran our algorithm to find a real zonotope invariant containing the real template G, but our algorithm failed. We also considered 5 uniformly randomly generated real valued templates to run our algorithm, but the search for sampling time invariant failed. Thus, complex zonotope based on eigenstructure is shown to be the better choice for verification on this example.

6 Experimental results

We implemented our algorithms and tested them on benchmark examples of NCS. We drew comparison with simple zonotope, i.e., having real valued generators and also the state-of-the-art tool SpaceEx [19]. For comparison with simple zonotope, we took the real template as the concatenation of real and imaginary parts of our complex template without repeated columns, and ran the same algorithm. In SpaceEx [19], the verification is performed by step-by-step forward reachability computation. In SpaceEx, we modeled NCS with uncertain sampling time as a hybrid system with linear guards and linear transitions. For convex optimization, we used CVX (version 2.2) with MOSEK solver (version 7.1) and Matlab 2020a 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.

6.1 Networked platoon of vehicles

This example is adapted from a model of a networked cooperative platoon of vehicles, which is presented as a benchmark in the ARCH workshop [29]. The platoon consists of three follower vehicles M_1, M_2 and M_3 along with a leader board ahead M_4. Each of the vehicles receives feedback input added to the acceleration, which depends on the communication of their relative distances, velocities and accelerations over a WLAN. The distance between a vehicle M_i and its next vehicle M_{i+1}, relative to a reference distances d_i^{ref}, is denoted by e_i. The acceleration of the leader vehicle is a_L which ranges between $[-9, 1](m/s)$. The state of the system is denoted by a 9-dimensional vector $x = [e_1, \dot{e}_1, \ddot{e_1}, e_2, \dot{e}_2, \ddot{e_2}, e_3, \dot{e}_3, \ddot{e_3}]$, which is the reference distance minus relative distances, the relative velocities and relative accelerations of the vehicles.

The disturbance input is the acceleration $a_L \in [-9, 1](m/s^2)$ of the leader board. In our adaptation, we consider that there can be uncertainty in the sampling period of the feedback input. The matrices of the NCS model are given below.

$$A = \begin{bmatrix} 0 & 1.0000 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1.0000 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1.6050 & 4.8680 & -3.5754 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1.0000 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1.0000 & 0 & 0 & -1.0000 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1.1936 & 3.6258 & -3.2396 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.0000 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1.0000 & 0 & 0 & -1.0000 \\ 0.7132 & 3.5730 & -0.0964 & 0.8472 & 3.2568 & -0.0876 & 1.2726 & 3.0720 & -3.1356 \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad C = \mathcal{I}_9 \qquad D = 0$$

$$F = \begin{bmatrix} 0 & 0 & 0 & -0.8198 & 0.4270 & -0.0450 & -0.1942 & 0.3626v - 0.0946 & \\ 0.8718 & 3.8140 & -0.0754 & 0 & 0 & 0 & -0.5950 & 0.1294 & -0.0796 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$V = \left\{ \begin{bmatrix} 0 \\ 0 \\ x \end{bmatrix} \mid x \in [-9, 1] \right\}, i.e., \mathrm{Re}\left(\mathcal{Z}\left(\begin{bmatrix} 0 & 0 & 1 \end{bmatrix}^T, \begin{bmatrix} 0 & 0 & -4 \end{bmatrix}^T, 5 \right) \right)$$

$$W = 0$$

Verification problem

For a given uncertainty of sampling period, the goal is to find the minimum possible reference distances $d^{ref} \in \mathbb{R}^3$ such that the vehicles should not collide, that is, $-e_i \leq d_i^{ref}$ $\forall i \in \{1, 2, 3\}$. For our experiment, we fix the lower bound on sampling period as $0.01(s)$ and verify the minimum possible bounds for various values of $\tau_{\max} \in \{0.012, 0.014, 0.016, 0.018s, 0.02\}\, s$. We used our Algorithm 1 to verify the bounds taking $K = 3$. We then used repeated the same algorithm with simple real valued zonotope containing concatenation of real and imaginary parts of the complex template. We also used SpaceEx to verify the bounds and draw a comparison based on the smallest value of the bound verified.

Results

For the different values of $\tau_{\max} \in \{0.012, 0.014, 0.016, 0.018, 0.02\}\, s$, we could verify finite values for $\left[d_1^{ref}, d_2^{ref}, d_3^{ref}\right]$ such that $-e \leq d^{ref}$ using our complex algorithm with complex zonotopes. The verified bounds are given in Table 1. The computation time is less than 310s for every bound and sampling time interval below. On the other hand, the simple zonotope version of our algorithm was unsuccessful in finding finite bounds. SpaceEx terminated unsuccessfully without being able to find any bounds on the reachable set.

Effect of increasing number of sampling times for eigenvectors. We increased K to 5 and got the following smaller bounds for $\tau_{\max} = 0.2s$: $d_1^{ref} = 40$m, $d_2^{ref} = 29m$ and $d_3^{ref} = 19m$. But the computation time increased to $656s$.

Remarks

In a continuous feedback model without switching based on digital sampling, the SpaceEx verification found the bounds $d^{ref} = (30, 30, 16)$ as reported in [29]. However, when there is intermittent switching of feedback input with uncertainty in the sampling time, SpaceEx could not find bounds in our experiment. Possibly the inductive step-by-step reachability algorithm

Table 1 Verified bounds for vehicle platoon.

$\tau_{\min} = 0.01s$

$\tau_{\max}$	d_1^{ref}	d_2^{ref}	d_3^{ref}
$0.012s$	$35m$	$26m$	$17m$
$0.014s$	$38m$	$27m$	$18m$
$0.016s$	$40m$	$29m$	$19m$
$0.018s$	40	$29m$	$19m$
$0.02s$	$44m$	$33m$	$22m$

used in SpaceEx could not overapproximate the reachable set resulting from switching of states in sampling time interval. Also, the simple zonotope version of our algorithm could not find a sampling time invariant. On the other hand, our complex zonotope containing eigenvectors in its template is able to represent a finite invariant for various levels of uncertainty in sampling time. Furthermore, the fact that use of simple zonotope failed to compute invariant but complex zonotope containing complex eigenvectors is successful shows that use of complex eigenvectors increases the chance of finding invariant in the presence of complex eigenstructure.

6.2 Self-balancing two wheeled robot

This example concerns a verification problem for the model of a self-balancing two wheeled robot called NXTway-GS1[1] by Yorihisa Yamamoto, which was presented in the ARCH workshop [23]. We consider the linearized networked control system model from the paper. The state of the plant is represented by a 6-dimensional vector $x_p = (\dot{\theta}, \theta, \dot{\rho}, \rho, \dot{\phi}, \phi)^T$, where θ is the average angle of the left and right wheel, ρ is the body pitch angle, ϕ is the body yaw angle, and the rest coordinates are their respective angular velocities. The output of the plant is represented by a 3-dimensional vector $(\dot{\rho}_{\text{out}}, \theta_{m_1}, \theta_{m_r})^T$ such that $y_p = C_p x_p$. The input to the plant u_p is a 2dimensional vector. The plant gets feedback input from a controller whose state is a 5-dimensional vector $x_c = \left(\theta_{err}, \theta_{ref}, \dot{\theta}_{ref\_lpf}, \rho, \theta_{lpf}\right)$. The variable θ_{err} is integration of error between $\dot{\theta}$ and θ_{ref}, and integration of $\dot{\theta}_{ref}$ is θ_{ref}. The low pass filter applied to $\dot{\theta}_{ref}$ is $\dot{\theta}_{ref\_lpf}$, body pitch angle is ρ, and the low pass filter applied to average valued of left/right motor angle is θ_{lpf}. The output of the controller is a 2-dimensional vector which is used to compute the feedback input. There is also a 2-dimensional unknown disturbance input.

In the benchmark paper [23], the output of the controller is sampled at 4ms to update the feedback input. In our experiment, we also consider the case where there is uncertainty in sampling period a possible disturbance in estimated output due to inaccurate sensors. The original model has an eleven dimensional continuous state of the plant (6) and controller (5) and 5-dimensional input. The trajectories of the system were unbounded along a 3-dimensional subspace of the system which can be found by diagonalization. We decoupled these unbounded directions and performed model reduction to obtain a lower dimensional system. For performing this decoupling, we used linear transformation of the state space based on block diagonalization. The transformed system has an eight dimensional continuous state, 2-dimensional controller output and four dimensional

[1] http://www.mathworks.com/matlabcentral/fileexchange/19147-nxtway-gs-self-balancing-two-wheeled-robot-controller-design

input. The matrices of the transformed NCS, disturbance input and output error sets are given below.

$$A = \begin{bmatrix} 0.0000 & 0.0000 & 0.1241 & 0.5638 & 0.5774 & -0.0000 & 0.0066 & 0.5774 \\ -0.0000 & -92.4135 & 0.0000 & 0.0000 & 0.0000 & -0.0000 & -0.0000 & 0.0000 \\ -363.0957 & 0.0000 & -127.3488 & 112.2606 & 85.8204 & -0.0714 & -2.2691 & 89.4013 \\ 256.3623 & 0.0000 & 64.4048 & -77.3066 & -45.5575 & -0.3242 & -17.1890 & -29.2897 \\ 172.3365 & 0.0000 & 34.5588 & -51.1441 & -26.0550 & 0.6640 & -17.2627 & -9.3837 \\ 0 & 0 & 0 & 0 & 0 & -1.0000 & 0 & 0 \\ 2.9915 & 0.0000 & 0.8811 & -0.3305 & 0.0320 & -0.0038 & -0.1829 & 0.2342 \\ 122.3365 & 0.0000 & 45.3074 & -2.8986 & -26.0550 & -0.3320 & 33.3025 & -59.3837 \end{bmatrix}$$

$$B = \begin{bmatrix} -0.0000 & -0.0000 & 0 & 0 \\ -51.3265 & 51.3265 & 0 & 0 \\ 144.4698 & 144.4698 & 0 & 0 \\ -76.6947 & -76.6947 & 0 & 0 \\ -43.8551 & -43.8551 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -0.8985 & -0.8985 & 0 & 0 \\ -43.8551 & -43.8551 & 0 & 0 \end{bmatrix} \qquad D = 0$$

$$C = 1000 \times \begin{bmatrix} -0.6895 & 0.0000 & 0.1537 & 0.6846 & 0.0151 & -0.0135 & 1.1696 & -0.6538 \\ -0.6895 & 0.0000 & 0.1537 & 0.6846 & 0.0151 & -0.0135 & 1.1696 & -0.6538 \end{bmatrix}$$

$$F = \begin{bmatrix} 0.0809 & 0 \\ 0 & 0.0809 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad V = [-100, 100] \times [-100, 100] \qquad W = [-1, 1]$$

Verification problem

The safety requirement is that the *body pitch angle* ρ of the robot should be bounded within $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$. The verification problem for NCS we consider in this paper is to find the largest value of upper bound $\tau_{\max}$ on sampling time such that the system is safe, given a lower bound $\tau_{\min} = 0.1(ms)$ and the safe set $\rho \in [-\frac{\pi}{2}, \frac{\pi}{2}]$. We used Algorithm 1 to verify safety bounds and subsequently find results for the above challenges based on complex zonotope. The same algorithm is repeated with a simple zonotope containing the concatenation of real and imaginary parts of our complex template. Concerning the experiment with SpaceEx using support functions, we tested with the octagon template and a template with 400 uniformly sampled support vectors distributed uniformly.

Results

Our algorithm based on complex zonotope could verify safety for $\tau_{\max} = 2$ms, given $\tau_{\min} = 0.1ms$. But SpaceEx could not find finite bounds on the reachable set for any value of uncertainty in sampling time. The simple zonotope based algorithm found a sampling time invariant, but its bounds were far over the threshold of safety, i.e., $\rho \in [-5.1\pi/2, 5.1\pi/2]$. The computation time for complex zonotope based algorithm is $153s$. We increased K to 7, but could not find any larger verified sampling time interval.

Remarks

The step-by-step reachability algorithm in SpaceEx possibly could not overapproximate resulting set of states from switching over the sampling time interval, due to which it failed to find bounds on reachable set. On the other hand, our complex zonotope containing eigenvectors in its template found bounded invariant which is within the limits of the safe set. Regarding the simple zonotope, although a sampling time invariant was found, the bounds were far over the threshold of safety. The reason complex zonotope is far more accurate than simple zonotope on this example is possibly that complex zonotope is geometrically more expressive, being able to encode nonlinear boundaries of invariants.

We saw that increasing K did not allow verification in a larger time interval. So, the strategy of sampling more time stamps for eigenvector template may not be the best strategy for improving the accuracy of verification. The problem remains open how to select sub-matrices for concatenation to the template to improve the accuracy of verification.

7 Conclusion

Given the pervasiveness of networked control systems with safety-critical applications, it is essential to develop verification algorithms for such systems in the presence of various possible inaccuracies in their execution. In this paper, we developed an algorithm to verify unbounded time safety of NCS with uncertain feedback sampling period, inaccurate output sensing and disturbance input. Our algorithm uses a novel set representation called complex zonotope that can capture convergence of forward reachable sets along eigenvectors and represent invariants. Complex zonotope is essentially an extension of simple zonotopes to the complex domain so as to efficiently compute invariants required by safety verification. Geometrically, their real projections represent a wider class of sets including some non-polytopic sets, while they retain the advantage of usual zonotope that the Minkowski sum and linear transformation can be computed efficiently. The practicality of our algorithm is demonstrated by successfully verifying benchmark examples with high dimensions (≥ 12 state+controller input variables), which the simple zonotope and another state-of-the-art tool failed to verify. An important direction for extension of this research is verifying NCS with non-linear differential equations and feedback. In this context, we need to find complex zonotope approximation of non-linear transformations and also conditions for checking invariance under non-linear transformation.

References

1 Arvind Adimoolam and Thao Dang. Augmented complex zonotopes for computing invariants of affine hybrid systems. In *International Conference on Formal Modeling and Analysis of Timed Systems*, pages 97–115. Springer, 2017.

2 Arvind Adimoolam and Thao Dang. Template complex zonotopes for stability and invariant verification. In *2017 American Control Conference (ACC)*, pages 2544–2549. IEEE, 2017.

3 Arvind S Adimoolam and Thao Dang. Template complex zonotopes: a new set representation for verification of hybrid systems. In *2016 International Workshop on Symbolic and Numerical Methods for Reachability Analysis (SNR)*, pages 1–2. IEEE, 2016.

4 Arvind S Adimoolam and Thao Dang. Using complex zonotopes for stability verification. In *2016 American Control Conference (ACC)*, pages 4269–4274. IEEE, 2016.

5 Santosh Arvind Adimoolam. *A Calculus of Complex Zonotopes for Invariance and Stability Verification of Hybrid Systems*. PhD thesis, Université Grenoble Alpes, 2018.

6 Assalé Adjé, Pierre-Loïc Garoche, and Alexis Werey. Quadratic zonotopes. In *Asian Symposium on Programming Languages and Systems*, pages 127–145. Springer, 2015.

7 Assalé Adjé, Stéphane Gaubert, and Eric Goubault. Coupling policy iteration with semi-definite relaxation to compute accurate numerical invariants in static analysis. In *European Symposium on Programming*, pages 23–42. Springer, 2010.

8 Mohammad Al Khatib, Antoine Girard, and Thao Dang. Stability verification of nearly periodic impulsive linear systems using reachability analysis. *IFAC-PapersOnLine*, 48(27):358–363, 2015.

9 Xavier Allamigeon, Stéphane Gaubert, and Eric Goubault. Inferring min and max invariants using max-plus polyhedra. In *International Static Analysis Symposium*, pages 189–204. Springer, 2008.

10 Xavier Allamigeon, Stéphane Gaubert, Eric Goubault, Sylvie Putot, and Nikolas Stott. A fast method to compute disjunctive quadratic invariants of numerical programs. *ACM Transactions on Embedded Computing Systems (TECS)*, 16(5s):1–19, 2017.

11 Xavier Allamigeon, Stéphane Gaubert, Nikolas Stott, Éric Goubault, and Sylvie Putot. A scalable algebraic method to infer quadratic invariants of switched systems. *ACM Transactions on Embedded Computing Systems (TECS)*, 15(4):1–20, 2016.

12 Matthias Althoff. 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*, pages 173–182, 2013.

13 Rajeev Alur. Formal verification of hybrid systems. In *Proceedings of the ninth ACM international conference on Embedded software*, pages 273–278, 2011.

14 Stephen Boyd, Stephen P Boyd, and Lieven Vandenberghe. *Convex optimization*. Cambridge university press, 2004.

15 Patrick Cousot and Nicolas Halbwachs. Automatic discovery of linear restraints among variables of a program. In *Proceedings of the 5th ACM SIGACT-SIGPLAN symposium on Principles of programming languages*, pages 84–96, 1978.

16 Jamal Daafouz, Pierre Riedinger, and Claude Iung. Stability analysis and control synthesis for switched systems: a switched lyapunov function approach. *IEEE transactions on automatic control*, 47(11):1883–1887, 2002.

17 Lei Ding, Qing-Long Han, Eyad Sindi, et al. Distributed cooperative optimal control of dc microgrids with communication delays. *IEEE Transactions on Industrial Informatics*, 14(9):3924–3935, 2018.

18 Mirko Fiacchini and Irinel-Constantin Morărescu. Set theory conditions for stability of linear impulsive systems. In *53rd IEEE Conference on Decision and Control*, pages 1527–1532. IEEE, 2014.

19 Goran Frehse, Colas Le Guernic, Alexandre Donzé, Scott Cotton, Rajarshi Ray, Olivier Lebeltel, Rodolfo Ripado, Antoine Girard, Thao Dang, and Oded Maler. Spaceex: Scalable verification of hybrid systems. In *Proc. 23rd International Conference on Computer Aided Verification (CAV)*, LNCS. Springer, 2011.

20 Antoine Girard. Reachability of uncertain linear systems using zonotopes. In *International Workshop on Hybrid Systems: Computation and Control*, pages 291–305. Springer, 2005.

21 Antoine Girard and Colas Le Guernic. Zonotope/hyperplane intersection for hybrid systems reachability analysis. In *International Workshop on Hybrid Systems: Computation and Control*, pages 215–228. Springer, 2008.

22 Michael Grant, Stephen Boyd, and Yinyu Ye. Cvx: Matlab software for disciplined convex programming, 2009.

23 Thomas Heinz, Jens Oehlerking, and Matthias Woehrle. Benchmark: Reachability on a model with holes. In *ARCH@ CPSWeek*, pages 31–36, 2014.

24 Laurentiu Hetel, Jamal Daafouz, and Claude Iung. Lmi control design for a class of exponential uncertain systems with application to network controlled switched systems. In *2007 American Control Conference*, pages 1401–1406. IEEE, 2007.

25 Laurentiu Hetel, Jamal Daafouz, Sophie Tarbouriech, and Christophe Prieur. Stabilization of linear impulsive systems through a nearly-periodic reset. *Nonlinear Analysis: Hybrid Systems*, 7(1):4–15, 2013.

26 Kyoung-Dae Kim and Panganamala R Kumar. Cyber–physical systems: A perspective at the centennial. *Proceedings of the IEEE*, 100(Special Centennial Issue):1287–1308, 2012.

27 Alexander B Kurzhanski and Pravin Varaiya. Ellipsoidal techniques for reachability analysis. In *International Workshop on Hybrid Systems: Computation and Control*, pages 202–214. Springer, 2000.

28 Michal Kvasnica. Minkowski addition of convex polytopes, 2005.

29 Ibtissem Ben Makhlouf and Stefan Kowalewski. Networked cooperative platoon of vehicles for testing methods and verification tools. In *ARCH@ CPSWeek*, pages 37–42, 2014.

30 Antoine Miné. The octagon abstract domain. *Higher-order and symbolic computation*, 19(1):31–100, 2006.

31 Stefan Pettersson and Bengt Lennartson. Hybrid system stability and robustness verification using linear matrix inequalities. *International Journal of Control*, 75(16-17):1335–1355, 2002.

32 Stephen Prajna and Ali Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *International Workshop on Hybrid Systems: Computation and Control*, pages 477–492. Springer, 2004.

33 Enric Rodríguez-Carbonell and Deepak Kapur. Automatic generation of polynomial invariants of bounded degree using abstract interpretation. *Science of Computer Programming*, 64(1):54–75, 2007.

34 Henrik Sandberg, Saurabh Amin, and Karl Henrik Johansson. Cyberphysical security in networked control systems: An introduction to the issue. *IEEE Control Systems Magazine*, 35(1):20–23, 2015.

35 Sriram Sankaranarayanan, Thao Dang, and Franjo Ivančić. Symbolic model checking of hybrid systems using template polyhedra. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 188–202. Springer, 2008.

36 Ashish Tiwari. Generating box invariants. In *International Workshop on Hybrid Systems: Computation and Control*, pages 658–661. Springer, 2008.

37 Yu-Long Wang and Qing-Long Han. Network-based modelling and dynamic output feedback control for unmanned marine vehicles in network environments. *Automatica*, 91:43–53, 2018.

38 Xian-Ming Zhang and Qing-Long Han. Network-based h∞ filtering using a logic jumping-like trigger. *Automatica*, 49(5):1428–1435, 2013.