Safety Verification of Networked Control Systems

Arvind Adimoolam and Thao Dang

Stability Verification of Networked Control Systems

Complex dynamics of Networked Control Systems

- Hybrid system models (mixed discrete and continuous)
- Uncertainty $\Rightarrow$ trajectory set computation for verification/controller synthesis

Set Representation for Verification

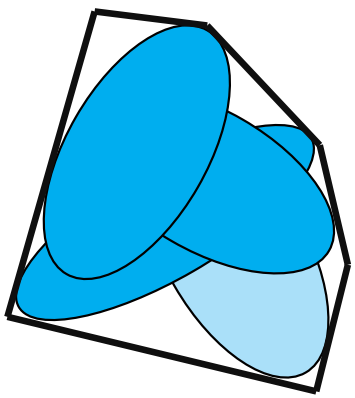
- Usual zonotope $\rightarrow$ Complex zonotope
  - Capture contraction along complex eigenvectors
- Complex zonotope $\rightarrow$ Template complex zonotope
  - Motivation: better approximation of reachable sets
  - Basic operations: linear transformation, Minkowski sum, support function
  - Checking inclusion : convex program
- Template complex zonotope $\rightarrow$ Augmented complex zonotope
  - Intersection with linear constraints

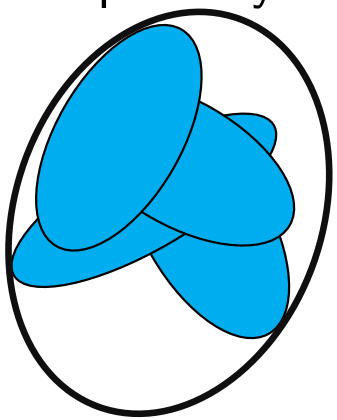
Set Representation for Verification

Need for set representations:

- To efficiently handle sets of possibly infinite solutions arising from non-determinism in dynamics

Set representation: A digital encoding of a possibly infinite set of states





Polytope

$\{x : Tx \leq d, x \in \mathbb{R}^n\}$

T: real matrix, d: vector of bounds.

Ellipsoid

$\{x : (x-c)^T P(x-c) \leq 1\}$.

P: Positive semi-definite matrix, c: real vector (center)

Requirements of a Set Representation

Goal: design set representation for efficiently computing reachable states

Typically required operations:
Linear transformation (e.g. continuous dynamics), Minkowski sum (e.g. input disturbance), Intersection with half-spaces (e.g. switching dynamics), e.t.c

- Accurate and fast computation: closure and low complexity under required set operations.

Plan

1. Usual zonotope $\rightarrow$ complex zonotope
   - Capture contraction along complex eigenvectors
2. Complex zonotope $\rightarrow$ Template complex zonotope
3. Stability verification of networked control systems

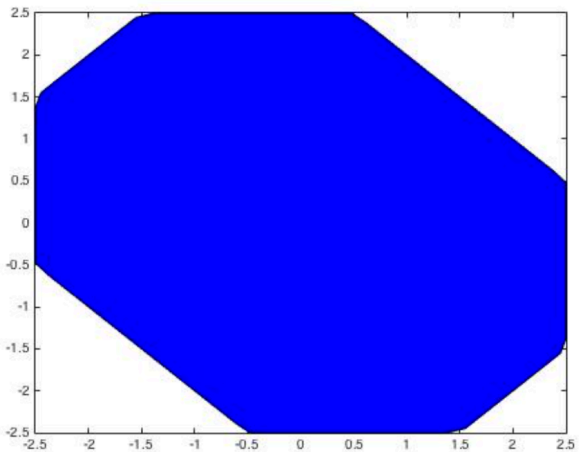
Usual Zonotope

A zonotope is a projection of higher dimensional hypercube onto lower dimensional space.

We consider a real matrix of generators V and center c

$$\mathcal{Z}(\mathcal{V}, c) := \{c + \mathcal{V}\zeta : \ \zeta \in [-1, 1]^m\}.$$

$$V = \begin{bmatrix} 1 & -1 & 0 & 0.5 \\ -1 & 0 & -1 & 0.5 \end{bmatrix}$$

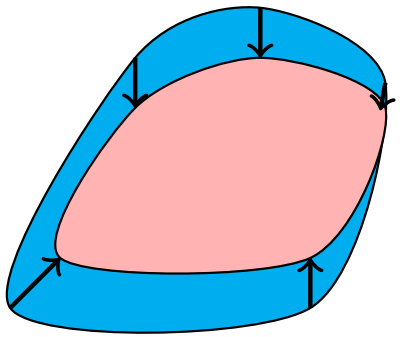


1. Linear transformation and Minkowski sum: Simple algebraic expressions
2. Advantage over polytope and ellipsoid

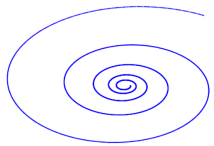
Drawback of Zonotopes for Computing Positive Invariants

Positive Invariant: Next reachable set contained inside the original set.

- Directions for convergence to an equilibrium can be encoded by complex valued eigenvectors.
- Usual zonotopes only have real eigenvectors as generators.



$a + \iota b: \quad a \neq 0 \quad b \neq 0.$



Let us consider a stable real matrix A whose real eigenvalues are μ and eigenvectors are $\mathcal{V}$. Then $A\left(\mathcal{Z}\left(\mathcal{V}, 0\right)\right) \subseteq \mathcal{Z}\left(\mathcal{V}, 0\right)$

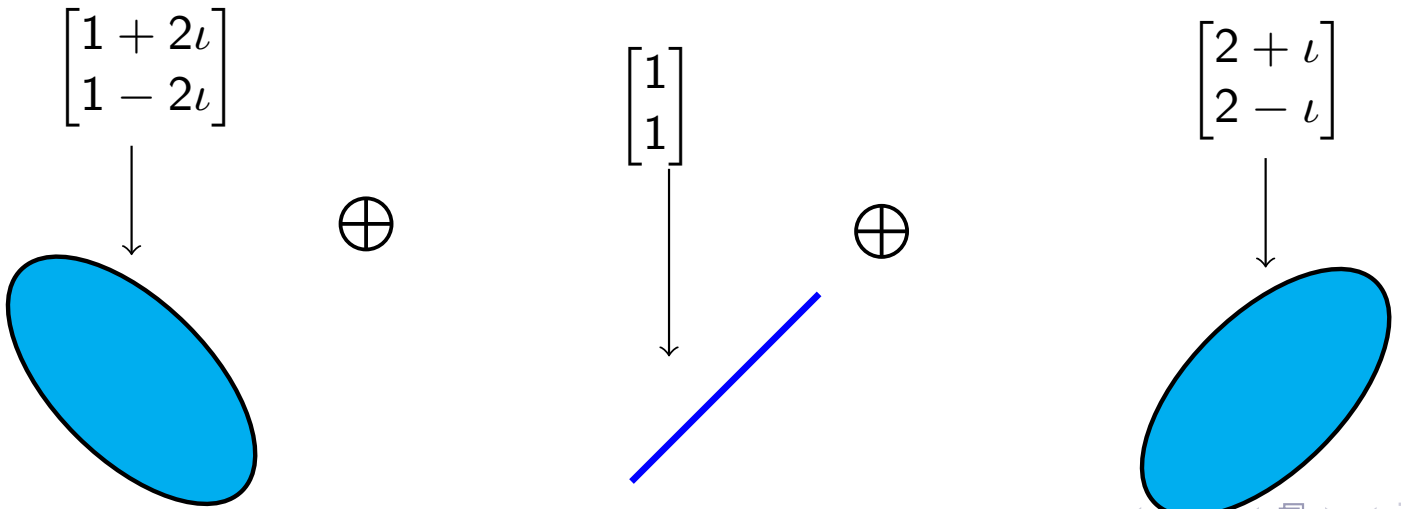
* We can not rely on above proposition when eigenvectors are complex.

Complex Zonotope: A New Set Representation

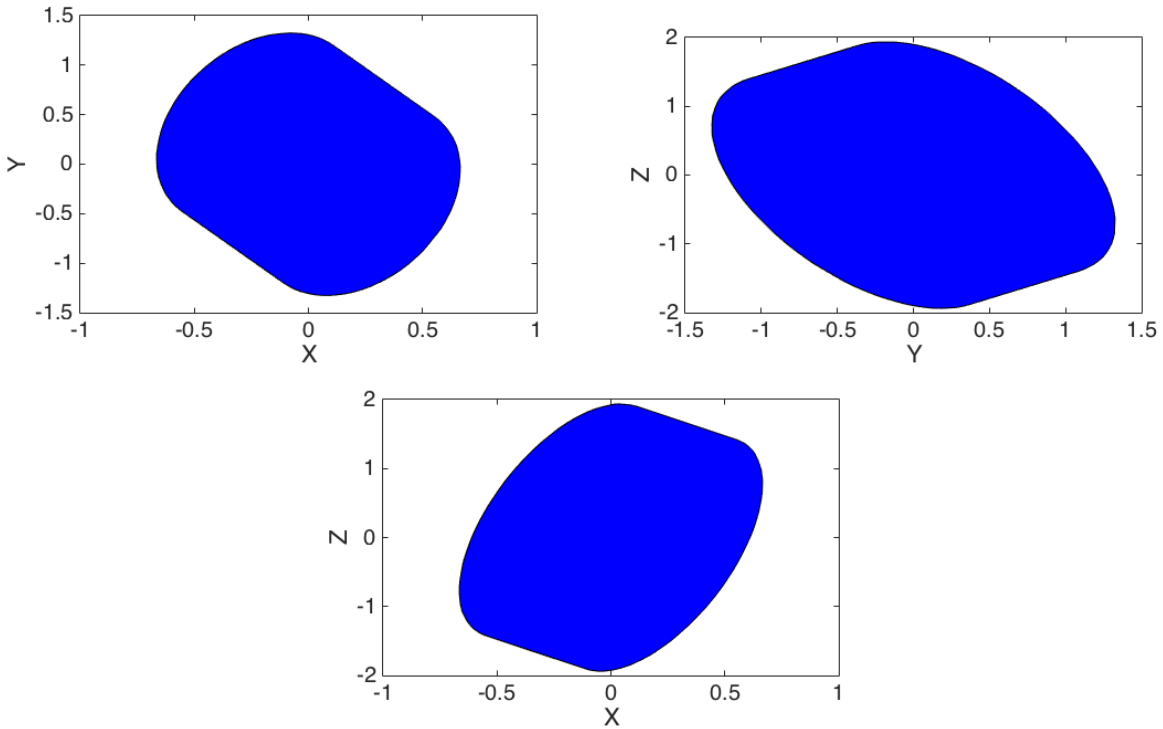
- Extend simple zonotope to complex numbers in a way that can capture contraction along complex vectors.
- Complex valued generators with complex combining coefficients whose absolute value ≤ 1.
- Geometrically, Minkowski sum of Ellipses and Line Segments.

Let us consider a complex matrix $\mathcal{V}$ and a real vector (center) c.

$$\mathcal{C}(\mathcal{V}, c) := \{\mathcal{V}\zeta + c : \ \zeta \in \mathbb{C}^m, \ \ \|\zeta\|_\infty \leq 1\}.$$



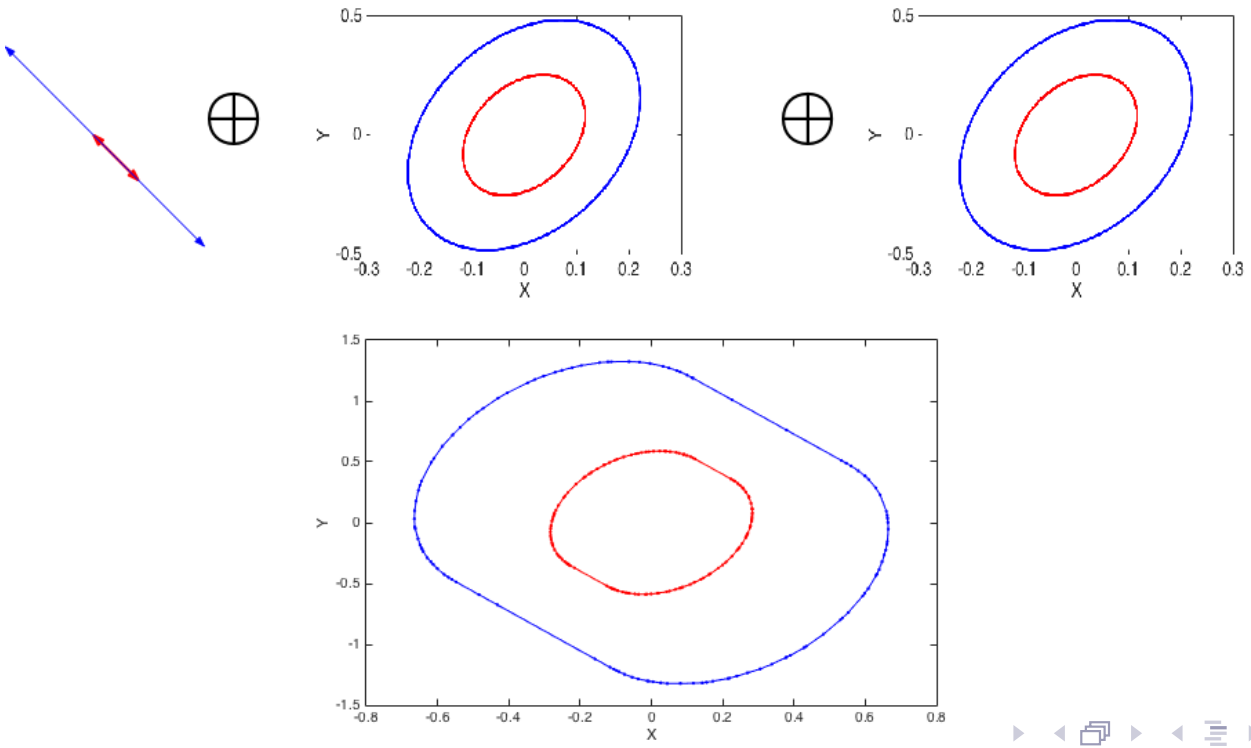
Non-polytopic Projection of Complex Zonotope



Complex Zonotopes: Ability to Capture Contraction along Complex Eigenvectors

Let A be a stable matrix having complex eigenvalues μ and complex eigenvectors $\mathcal{V}$

$$A\left(\mathcal{C}\left(\mathcal{V},0\right)\right) \subseteq \mathcal{C}\left(\mathcal{V},0\right).$$



Plan

1. Usual zonotope $\rightarrow$ Complex zonotope
2. Complex zonotope $\rightarrow$ Template complex zonotope
   - Motivation: better approximation of reachable sets
   - Basic operations: linear transformation, Minkowski sum, intersection
   - Checking inclusion: convex program
3. Stability verification of networked control systems

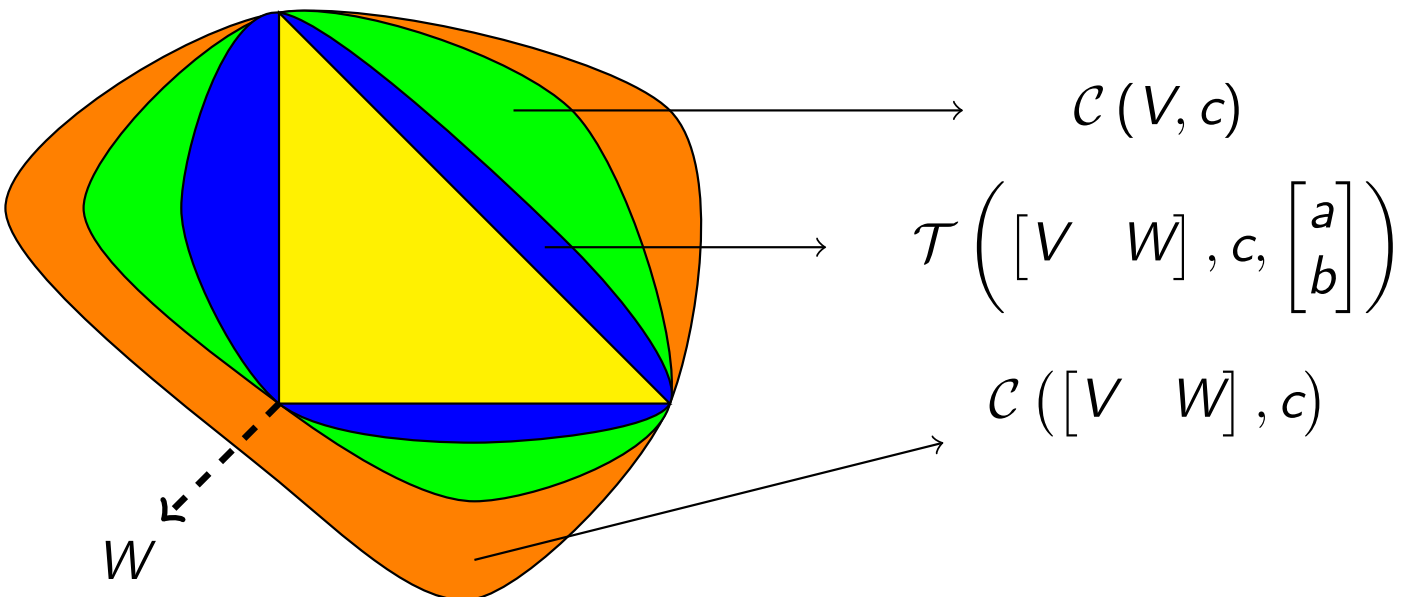
Template Complex Zonotope: Definition

Variable bounds on absolute values of combining coefficients.

$\mathcal{V} \in \mathbb{M}_{n\times m}(\mathbb{C})$: template, $\boxed{s \in \mathbb{R}^m_{\geq 0}}$: scaling factors, $c \in \mathbb{R}^n$: center.

$$\mathcal{T}(\mathcal{V}, c, s) = \{\mathcal{V}\zeta + c : \ |\zeta_i| \leq s_i \ \forall i \in \{1, ..., m\}\}.$$

- Add more generators and adjust scaling factors to find better approximations.



Basic Operations: Template Complex Zonotope

1. $A\mathcal{T}(\mathcal{V}, c, s) = \mathcal{T}(A\mathcal{V}, Ac, s)$.
2. $\mathcal{T}(\mathcal{V}, c, s) \oplus \mathcal{T}(\mathcal{V}', c', s') = \mathcal{T}\left(\begin{bmatrix}\mathcal{V} & \mathcal{V}'\end{bmatrix}, c + c', \begin{bmatrix}s \\ s'\end{bmatrix}\right)$.

- Above are affine functions of center and scaling factors.

Checking Inclusion

Generally, checking inclusion between complex zonotopes requires non-convex optimization. Inclusion of a point. Consider a point $x \in \mathbb{C}^n$. Then $x \in \mathcal{T}(\mathcal{V}, c, s) \subset \mathbb{C}^n$ if and only if all of the following is collectively true.

$$\exists \zeta \in \mathbb{C}^m :$$
$$\mathcal{V}\zeta = x - c \tag{1}$$
$$|\zeta| \leq s. \tag{2}$$

Exact inclusion between template complex zonotopes. Consider $\mathcal{V} \in \mathbb{M}_{n\times m}(\mathbb{C})$ and $\mathcal{V}' \in \mathbb{M}_{n\times r}(\mathbb{C})$. The inclusion $\mathcal{T}(\mathcal{V}', c', s') \subseteq \mathcal{T}(\mathcal{V}, c, s)$ holds if and only if

$$\sup_{\{\zeta' \in \mathbb{C}^r : |\zeta'| \leq s'\}} \inf_{\{\zeta \in \mathbb{C}^m : \mathcal{V}\zeta = \mathcal{V}'\zeta' + c' - c\}} \max_{i=1}^{m} (|\zeta_i| - s_i) \leq 0 \tag{3}$$

Checking Inclusion

Generally, checking inclusion between complex zonotopes requires non-convex optimization. $\rightarrow$ we propose a convex relaxation that works well in practice.

Definition ($\mathcal{T}(\mathcal{V}', c', s') \sqsubseteq \mathcal{T}(\mathcal{V}, c, s)$)

$$\exists X \in \mathbb{M}_{m \times r}(\mathbb{C}), y \in \mathbb{C}^m \text{ such that}$$
$$\mathcal{V}X = \mathcal{V}' \operatorname{diag}(s'), \quad \mathcal{V}y = c' - c$$
$$\sup_{i=1}^{m} \left(|y_i| + \sum_{j=1}^{r} |X_{ij}| - s_i \right) \leq 0.$$

Result: $\sqsubseteq \implies \subseteq$.

- $\sqsubseteq$: Second order conic constraints (convex constraints) on center and scaling factors.

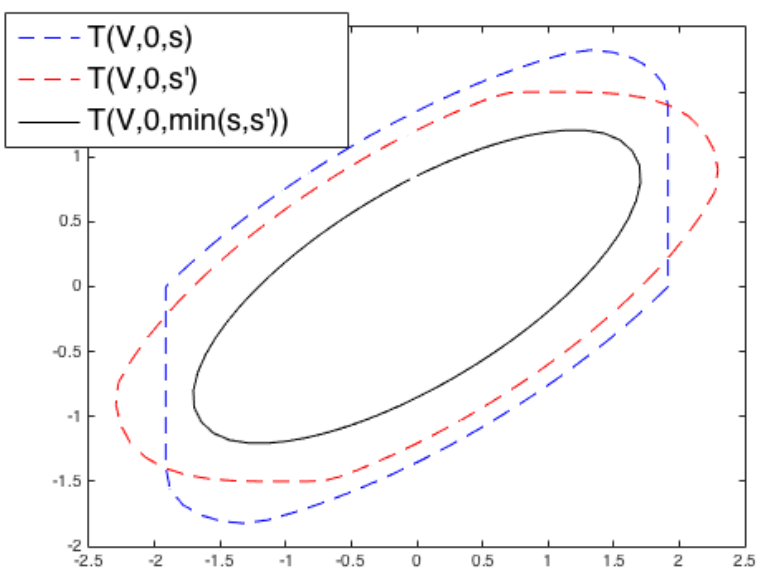
Intersection between Complex Zonotopes

- Closed for common invertible template

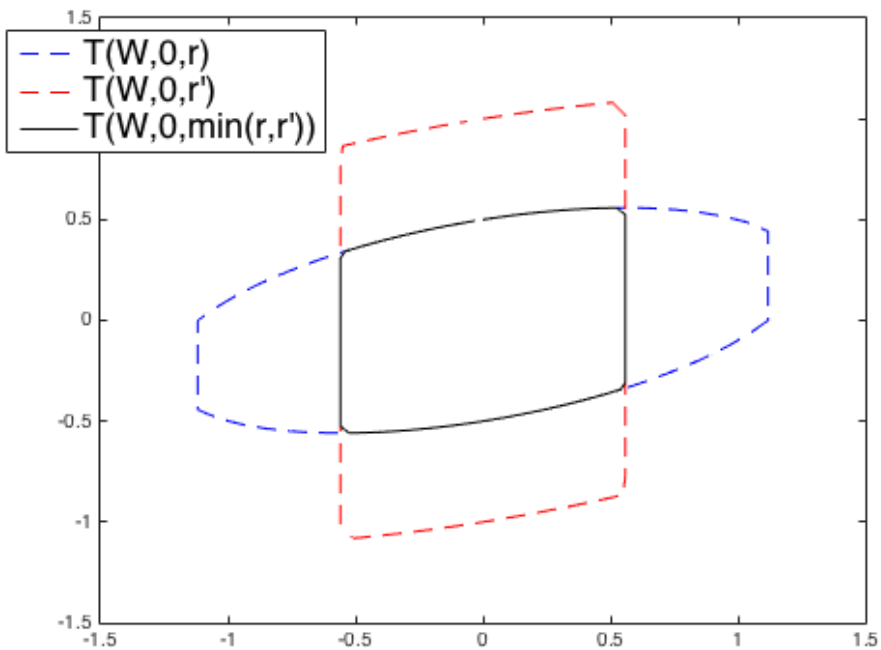
Let us consider a invertible matrix $\mathcal{V}$

$$\mathcal{T}(\mathcal{V}, c, s) \bigcap \mathcal{T}(\mathcal{V}, c, s') = \mathcal{T}(\mathcal{V}, c, s \bigwedge s').$$

Non-closure for a non-invertible template.



Closure for an invertible template.



Comparison with Existing Set Representations

Set representation	Linear transformation	Minkowski sum	Intersection with half-space	Positive Invariant (non-empty interior) stable invertible linear transformation
Convex polytope H-representation	Efficient only for invertible matrix	More than exponential complexity	Efficient	Maximum complexity of encoding not bounded
Zonotope	Efficient	Efficient	Not closed	May not exist
Ellipsoid	Efficient	Not closed	Not closed	Efficient encoding
Polynomial sub-level set	More than exponential complexity	More than exponential complexity	Efficient	Efficient encoding
Template Complex Zonotope	Efficient	Efficient	Not closed	Efficient encoding

Plan

1. Usual zonotope → Complex zonotope
2. Complex zonotope → Template complex zonotope

Template complex zonotope → Augmented complex zonotope

- Intersection operation for discrete transitions

3. Stability verification of networked control systems

Augmented Complex Zonotope: Motivation

To handle discrete transitions, we compute intersection with guards. But intersection is not closed.

Earlier solutions: extensions of real zonotope

- Constrained Zonotope [Scott *et al.* 2016], Constrained Affine set [Ghorbal *et al.* 2010]
- Allow additional linear constraints on coefficients.
- Using this idea for complex zonotopes is not tractable

$\Rightarrow$ Our solution: Augmented complex zonotope

Augmented Complex Zonotope : Definition

- Minkowski sum of template complex zonotope and interval zonotope.

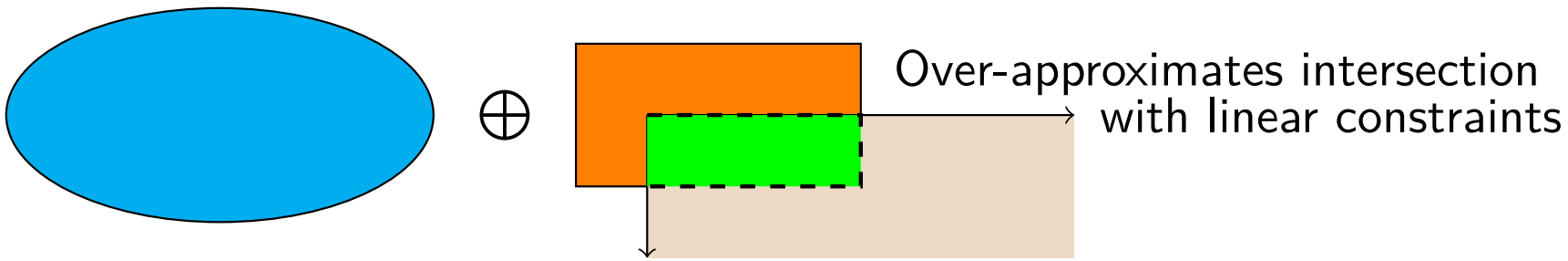
Interval Zonotope: $\mathcal{I}(\mathcal{W}, l, u)$

$$\{\mathcal{W}\zeta : \zeta \in \mathbb{R}^k,\ l \leq \zeta \leq u\}.$$

Template Complex Zonotope $\oplus$ Interval Zonotope

$$\mathcal{T}(\mathcal{V}, c, s) \oplus \mathcal{I}(\mathcal{W}, l, u).$$

Template complex zonotope



Captures contraction
along complex vectors

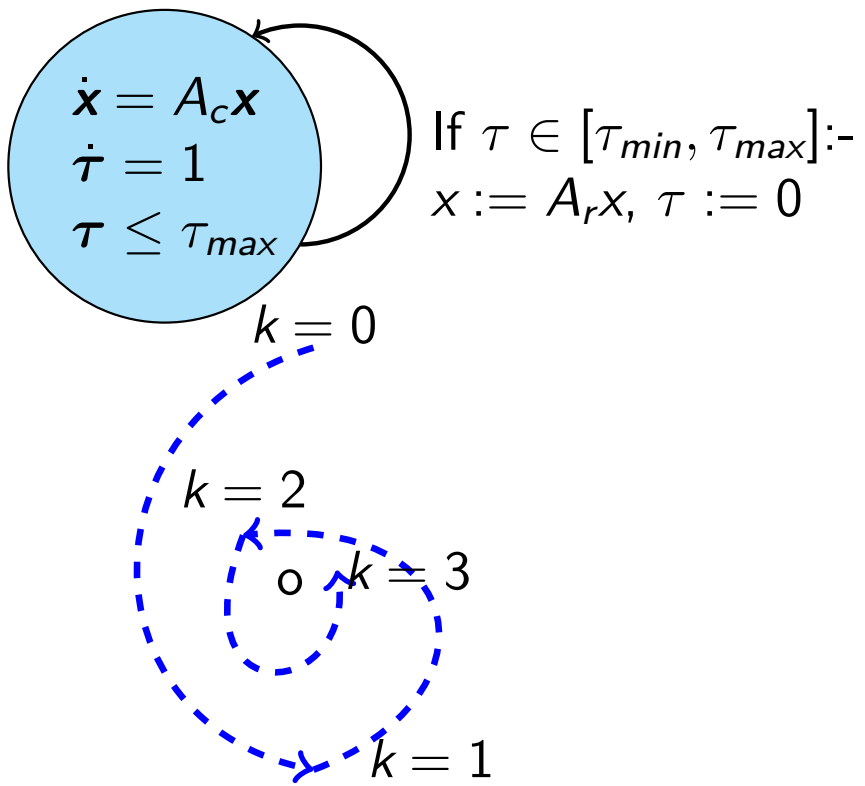
Plan

1. Usual zonotope → Complex zonotope
2. Complex zonotope → Template complex zonotope
3. Stability verification of networked control systems

Networked Control Systems

- Networked control system (plant and controller) with sensors (sampling) and actuators (impulse)
- Modeled as Nearly periodic linear impulsive system

1. Linear impulse (actuation) applied to sampled state of continuous time linear system E.g.
2. Time between successive sampling is bounded.



Global exponential stability (GES)

Exists $\lambda \in [0, 1)$ and $c > 0$ such that $\forall\ \mathbf{x}_0, \in \boldsymbol{R}^n,\ k \in \boldsymbol{Z}_+$

$$||\mathbf{x}_k|| \leq c\lambda^k ||\mathbf{x}_0||$$

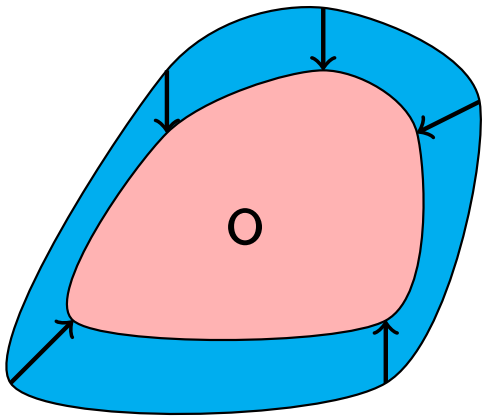
Set Contraction and Stability Verification

$H_\tau = e^{A_c \tau} A_r$. Contractive C-set [Fiacchini et al 2014]:

Compact and convex set Ψ:

1. Origin is interior point.
2. Contraction: $\exists\ \lambda \in [0, 1)$: $\forall \tau \in [\tau_{min}, \tau_{max}]$

$$H_\tau \Psi \subseteq \lambda \Psi.$$



Existence of contractive C-set $\Leftrightarrow$ GES.

- Find contractive C-set to verify GES.

Stability Verification Using Complex Zonotope

2 stages:

1. Synthesize a candidate complex zonotope.
2. Verify contraction of candidate complex zonotope.

Synthesizing Candidate Complex Zonotope

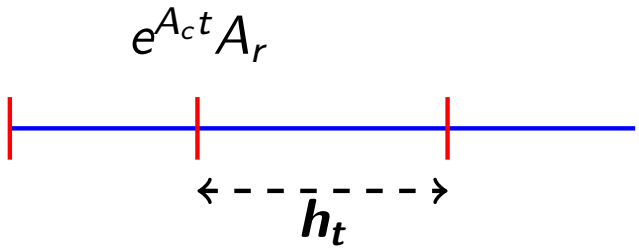
1. Collect eigenvectors of K-uniformly sampled reachability operators as template.

Eigenvectors of $e^{A_c t} A_r$:
t is uniformly sampled

2. Synthesize scaling factors such that we get
   1. λ-contractive complex zonotope
   2. contains unit box containing origin (C-set)

Verifying Contraction w.r.t All Reachability Operators

1. Derive contraction bound in a small neighborhood of a reachability operator using known operations on complex zonotopes.
   - Requires convex optimization.
2. Dynamically divide sampling intervals into small sub-intervals while verifying contraction bound < 1.



h_t = Maximum interval at t for which contraction bound is less than 1.

Benchmark: Networked Control System

Benchmark from [Wittenmark *et al.* 2002]

- Lower bound on the transmission period: 0.08

Find upper bound t_{max} on transmission period such that system is GES

Reference	t_{min}	t_{max}
Value recommended in [Wittenmark *et al.* 2002]	0.08	0.22
NCS toolbox [Bauer *et al.* 2012]	0.08	0.4
Template complex zonotope	0.08	0.58

NXT-Lego Robot Model

Benchmark example published in ARCH 2014 [Heinz et. al 2014]

Lego NXT self-balancing robot by Medelen8/CC-BY-SA-3.0

- Sampled data Networked Control System
- Controller input has saturation on 2 controller inputs: hybrid behavior.

$$\begin{bmatrix} \mathbf{x}(t+1) & \mathbf{y}(t+1) \end{bmatrix}^T = F_1\mathbf{x}(t) + F_2 sat(\mathbf{y}(t)) + F_3\mathbf{u}(t)$$

Saturated: $sat(y_i) = max(-\delta d_p, min(y_i, \delta d_p)),\ \forall i \in \{1,2\}$, where $\delta = 100$ and $d_p = 0.0807$. Unsaturated: $sat(y_i) = y_i$

NXT-Lego Robot Model: Verification Problem

The state of the plant: 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.
The output of the plant: 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 2 dimensional vector.
The controller state is a 5-dimensional vector $x_c = \theta_{err}, \theta_{ref}, \dot{\theta}_{ref\_lpf}, \rho, \theta_{lpf}$.
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 $\dot{\theta}_{ref\_lpf}$.
There is also a 2-dimensional unknown disturbance input.

Verify bounds on body pitch angle

After transformation to decouple unbounded directions, we obtained

Complexity

- Saturated: 9 dimensional, 1 location, 9 edges.
- Unsaturated: 9 dimensional linear system.

NXT-Lego Robot Model: Results

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

Method		$\|\psi\| \leq$	Comp. time (s)
SpaceEx	octagon template	UB	NT
	400 support vectors	UB	NT
Suggested in [Heinz et. al. 2014]		1.39	n/a
ACZ invariant		1.29	4

Unsaturated robot model: results

Method		$\|\psi\| \leq$	Comp. time (s)
SpaceEx	octagon template	UB	NT
	400 support vectors	UB	NT
Suggested in [Heinz *et al.*. 2014]		$1.571 - \epsilon : \epsilon > 0$	n/a
ACZ invariant		1.13	45

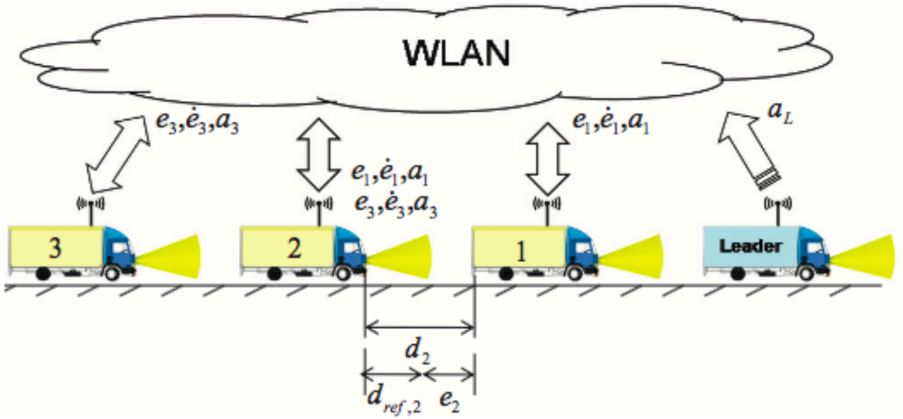
Saturated robot model: results

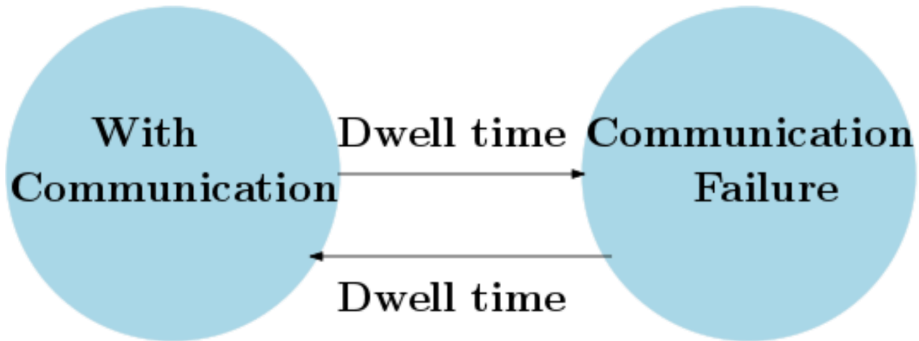
Remarks

- Model has complex eigenstructure, some eigenvalues have magnitude close to 1.
- Complex Zonotope uses complex eigenstructure: better accuracy.

Networked Vehicle Platoon

Benchmark 2014 ARCH Workshop: [Makhlouf *et al.* 2014]





- Continuous disturbance input: the acceleration of the leader board

Networked Platoon Verification Problem

Verify reference distances between vehicles such that they do not collide.

Two cases

1. Slow switching: Minimum dwell time 20 s. 9 dimensional, 2 locations, 4 edges.
2. Fast switching: Integer dwell times. 9 dimensional, 2 locations, 2 edges.

Networked Platoon: Results

Method		Slow switching				Fast switching			
		$-e_1 \leq$	$-e_2 \leq$	$-e_3 \leq$	Comp. time (s)	$-e_1 \leq$	$-e_2 \leq$	$-e_3 \leq$	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 [Makhlouf *et al.* 2014]		25	25	10	n/a	n/a	n/a	n/a	n/a
ACZ invariant		28	26	12	12	46	54	57	12.6

Remarks

- **Fast switching model** is less stable than **slow switching model**
- Since **complex zonotope** used eigenstructure: better accuracy on less stable model

Summary

1. Complex zonotope representations that
   - capture continuous dynamics contractions
   - efficient operations for discrete dynamics
2. Improve the state of the art of verification
   1. linear invariance
   2. stability
3. Implementation and successful experimentation on benchmarks

Current work

1. Scheduling of NCS under safety constraints (by estimating the sampling time that maintains both stability and safety)

Thank you