A Calculus of Complex Zonotopes for Invariance and Stability Verification of Hybrid Systems

Santosh Arvind Adimoolam

Models of hybrid systems, that describe the system dynamics as an interaction between continuous and discrete variables, pose a significant challenge for formal verification. Verification of some of the properties of these systems, like safety and stability, usually requires computing the set of reachable states of the system. For hybrid systems that have differential equations, exact computation of the reachable set is undecidable [5], except in particular cases [14]. Even in a simpler case like a discrete time affine hybrid system, the exact reachable set at any given time is a union of sets whose number is exponential in the number of time steps. An alternative is find a sufficiently accurate over-approximation of the infinite set of reachable states. To do so, we need to represent an infinite set of states symbolically by a *set representation*, which can be efficiently manipulated for the computation of the desired over-approximation. Some examples of a set representation are *convex polyhedron*, represented by either linear inequalities [6, 17, 7] or a convex hull of a finite set of points [13]; *ellipsoid* [3, 12], represented by a positive semi-definite matrix and a center; *polynomial sub-level sets* [2, 16] ; etc. In numerical abstract interpretation, a set representation is usually an *abstract domain*, which is a lattice with an abstraction and a concretization map [11].

1 Motivation

We consider the problem of efficiently computing a sufficiently accurate over-approximation of the unbounded time reachable set that is useful for verifying properties like invariance and stability. The unbounded time reachable set is usually approximated as a *positive invariant*, which is a set of states whose next set of reachable states is contained within itself. The potentiality of a set representation for efficient computation of a positive invariant of a hybrid system is affected by the following characteristics. (i) Closure of the set representation under set operations like linear transformation, Minkowski sum, intersection and inclusion-checking, etc, and efficient computation of the same. (ii) Existence of a positive invariant for the system that can be encoded by the set representation. (iii) Efficient encoding of the positive invariant by the set representation. Well known set representations for computing reachable sets have some of the above characteristics, but not all. For example, polytopes have the advantage that they are closed under linear transformation, Minkowski sum and intersection and for a stable linear transformation, there exists a polytopic invariant. However, the Minkowski sum operation is costly because it can lead to a quadratic increase in the number of vertices and an exponential increase in the number of faces. Also, the number of faces of a polytopic positive invariant for a stable linear system can be arbitrarily large. Ellipsoids have the advantage that they are closed under linear transformation and can also efficiently represent the positive invariant of a stable linear transformation. But ellipsoids are not closed under Minkowski sum. Recently work computes the over-approximation of the Minkowski sum of ellipsoids by a minimum volume ellipsoid [4]. Still, there can be significant approximation error in the ellipsoidal approximation of the Minkowski sum.

Real zonotope, its usefulness and drawback. Zonotope [9] is yet another set representation, which is specified as a linear combination of real vectors and a center, such that the absolute values of the combining coefficients are bounded within unity. Geometrically, a zonotope is the Minkowski sum of line segments and hence a type of polytope. Zonotopes have also been extended to the more general quadratic zonotopes [1], which is a quadratic function of real valued intervals. Zonotopes have the advantage that they are efficiently closed under linear transformation and Minkowski sum operations. Therefore, they have been successfully applied to the computation of bounded time reachable sets of uncertain continuous linear systems [9] and affine hybrid systems with simple switching [15, 10]. But for over-approximation of the *unbounded time reachable set by a positive invariant*, real zonotopes have the have the following drawback. We can not guarantee the existence of real zonotope which is a positive invariant, for the case of a stable linear transformation having complex eigenvalues. When the eigenvectors of a stable linear transformation are real valued, then collecting the eigenvectors of the matrix among the generators of the zonotope gives a positively invariant real zonotope. However, this result does not hold when the eigenvectors have complex values, i.e., have non-zero imaginary and real parts.

2 Main Contribution

Complex zonotope. To address the above drawback of real zonotopes, we extend them to the complex valued domain to yield a set representation called *complex zonotope.* A basic representation of a complex zonotope, which is a straightforward extension of the real zonotope, is a linear combi-

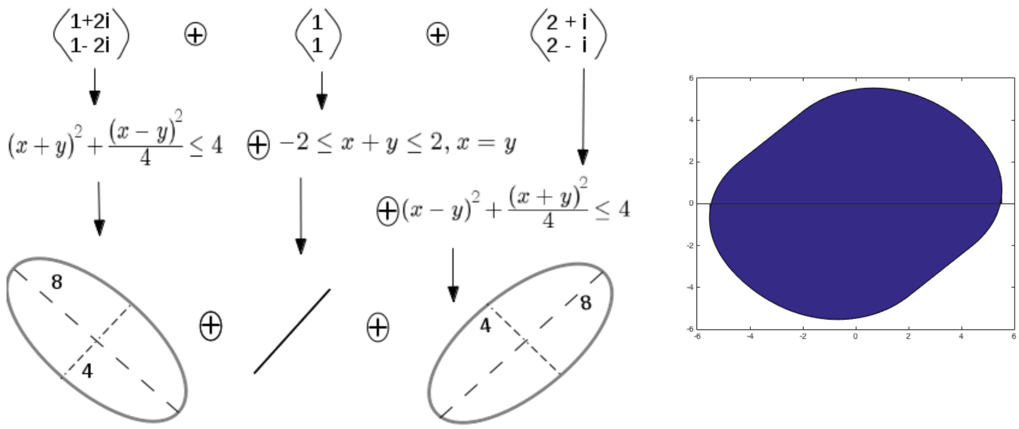

Figure 1: Figure of a complex zonotope

nation of complex valued vectors with complex combining coefficients, whose absolute values are bounded within unity. We show that a complex zonotope captures contraction along the complex valued eigenvectors of a linear transformation, which relates to existence of a positively invariant complex zonotope. The real projection of a complex zonotope can represent not only Minkowski sums of line segments, but also some ellipsoids. Hence, they can represent non-polyhedral sets as well as polytopic zonotopes. They are different from quadratic zonotopes [1], because while the latter is a quadratic function of real valued intervals, a complex zonotope is a complex linear combination of circles in the complex plane.

Template complex zonotope. To find more accurate approximations of a given set using a basic representation of a complex zonotope, we can not simply add more generators because it only increases the size of the complex zonotope. Moreover, adding generators can violate the positive invariance of the complex zonotope. An alternative way of refining the complex zonotope is to modify the measure of contribution of each generator to the size of the set. In this regard, we propose the more general *template complex zonotope* representation, where the absolute values of combining coefficients have variable bounds called scaling factors. The scaling factors can be adjusted to find better over-approximations. Furthermore, it allows adding arbitrary generators to the collection of generators, called the *template*, because the scaling factors can adjusted to any value equal to or greater than zero.

Advantage over other set representations: Just like simple zonotopes, template complex zonotopes are also closed under linear transformation and Minkowski sum operations and the resultant complex zonotopes can be computed efficiently. This is an advantage over ellipsoids which are not closed under Minkowski sum. Additionally, we show that template complex zonotope can efficiently represent a positive invariant for a linear transformation, by collecting the eigenvectors of the linear transformation as vectors in the template. This is an an advantage over real zonotopes, where we can not guarantee if a positive invariant, represented as a real zonotope, exists when the eigenvectors are complex valued. This is also an advantage over polytopes, where the representation size of a positive invariant as a polytope can be arbitrarily large.

Inclusion-checking: We propose a sufficient condition for checking inclusion between template complex zonotopes, expressed as a second-order conic (convex) constraint on the scaling factors and other auxiliary variables. This condition is useful in practice, which we demonstrate through our experiments in invariance and stability verification on some benchmark examples.

Augmented complex zonotope. Template complex zonotopes are not closed under intersection with sub-level sets of linear inequalities. This is also a drawback of real zonotopes. Previous work addressed this drawback for real zonotopes by allowing linear constraints on the combining coefficients, in more general representations like constrained affine sets [8] and *constrained zonotopes* [18]. But we face the following problem if we were to emulate these approach for complex zonotopes. The absolute value bounds on combining co-coefficients, which are quadratic functions, are necessary because they capture the contraction along complex valued eigenvectors of a linear transformation. Consider that we additionally define linear constraints on the complex valued combining co-coefficients to reason about intersection. Then the problem of finding a reasonable convex-relaxation for inclusion-checking between elements in the resultant set representation, which works well in practice, seems intractable. Instead, we define a representation called *augmented complex zonotope*, which is geometrically equivalent to a complex zonotope, but whose representation is more general and allows efficient computation of a non-trivial over-approximation of the intersection with a class of linear constraints. The over-approximation is computed as a simple algebraic expression of the parameters of the augmented complex zonotope. The augmented complex zonotope representation is motivated by the constrained affine sets [8] abstract domain. But the difference is that while a constrained affine set is geometrically not a zonotope, an augmented complex zonotope is geometrically equivalent and can be converted efficiently to the template complex zonotope. Therefore, we can efficiently check-inclusion between augmented complex zonotopes using the condition for checking-inclusion between template complex zonotopes. In the course of the derivation of this result about intersection, we also find a general mathematical result about intersection of Minkowski sum of convex sets with another convex set.

Invariance verification. Henceforth, we derive a second order conic program for checking the invariance of linear constraints for a discrete time affine hybrid system. The fact that a complex zonotope can both capture the contraction along complex eigenvectors and also efficiently represent linear transformation and Minkowski sum makes it an efficient set representation for unbounded time safety verification. We demonstrate the efficiency of the safety verification approach by implementing on some benchmark examples and comparing with the SpaceEx tool [7] and available results for previous approaches.

Stability verification of nearly periodic linear impulsive systems. Our analysis of template complex zonotopes for the case of discrete time switched linear systems is extended to verify stability of *nearly periodic linear impulsive systems*. The efficiency of our approach to stability verification is demonstrated by our experiments on some benchmark experiments. We obtain either larger or competitive bounds on the maximum uncertainty in sampling times compared to previous approaches.

3 Organization

The dissertation contains five main chapters and a conclusive chapter. In Chapter 1, we briefly discuss the use of set representation for computing reachable sets of hybrid systems and the desirable characteristics of a good set representation. In light of these characteristics, we provide a short review of some set representations that discusses their advantages and drawbacks. Then we review simple/real zonotopes and the commonly used operations on them in reach set computation. We also review the definitions polynomial and constrained zonotopes, which are previously known extensions of the simple zonotope. Then we shall describe the shortcoming of the real zonotope in computing a positive invariant.

In Chapter 2, we introduce the complex zonotope set representation that addresses the drawback of real zonotope described in the previous chapter. We define the basic representation of a complex zonotope and state a result about how a complex zonotope can efficiently represent a positive invariant for a stable linear transformation based on the eigenstructure. Next we define the more general template complex zonotope representation, which permits a way of refining a complex zonotope while approximating a given set. We discuss operations on template complex zonotopes that are used in reach set computation and derive a second order conic program for checking inclusion between template complex zonotopes. Using the results, we derive a second order conic program for unbounded time safety verification of linear systems and illustrate it with an example.

In Chapter 3, we introduce augmented complex zonotopes for computing non-trivial intersection with a class of sub-level sets of linear inequalities called sub-parallelotopes. Apart from the intersection, we discuss other operations on augmented complex zonotope used in the computation of reachable sets. Also, we state a second order conic program for checking inclusion between augmented complex zonotopes.

In Chapter 4, we apply augmented complex zonotopes for unbounded time safety verification of affine hybrid systems. We derive a second order conic program for checking safety, which is based on computing a suitable positively invariant augmented complex zonotope. We implement the approach on some benchmark examples to demonstrate its efficiency.

In Chapter 5, we apply template complex zonotopes for verifying exponential stability of linear impulsive systems with sampling time uncertainty. We discuss a procedure for stability verification, which consists of synthesizing a possibly contractive template complex zonotopes and verifying their contraction. We implement this procedure on some benchmark examples to demonstrate its efficiency.

The concluding remarks are stated in Chapter 6.

References

[1] Assalé Adjé, Pierre-Loïc Garoche, and Alexis Werey. Quadratic zonotopes - an extension of zonotopes to quadratic arithmetics. In *Programming Languages and Systems - 13th Asian Symposium, APLAS 2015, Proceedings*, pages 127–145, 2015.

[2] Assalé Adjé, Stéphane Gaubert, and Eric Goubault. Coupling policy iteration with semi-definite relaxation to compute accurate numerical invariants in static analysis. In *Programming Languages and Systems, 19th European Symposium on Programming, ESOP 2010, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2010, Paphos, Cyprus, March 20-28, 2010. Proceedings*, pages 23–42, 2010.

[3] Xavier Allamigeon, Stéphane Gaubert and" Nikolas Stott, Eric Goubault, and Sylvie Putot. A scalable algebraic method to infer quadratic invariants of switched systems. *ACM Trans. Embedded Comput. Syst.*, 15(4):69:1–69:20, 2016.

[4] 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):166, 2017.

[5] Rajeev Alur, Costas Courcoubetis, Nicolas Halbwachs, Thomas A Henzinger, P-H Ho, Xavier Nicollin, Alfredo Olivero, Joseph Sifakis, and

Sergio Yovine. The algorithmic analysis of hybrid systems. *Theoretical computer science*, 138(1):3–34, 1995.

[6] 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. ACM, 1978.

[7] 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.

[8] Khalil Ghorbal, Eric Goubault, and Sylvie Putot. A logical product approach to zonotope intersection. In Tayssir Touili, Byron Cook, and Paul Jackson, editors, *Computer Aided Verification: 22nd International Conference, CAV 2010, Edinburgh, UK, July 15-19, 2010. Proceedings*, 2010.

[9] Antoine Girard. Reachability of uncertain linear systems using zonotopes. In *Hybrid Systems: Computation and Control, 8th International Workshop, HSCC 2005, Zurich, Switzerland, March 9-11, 2005, Proceedings*, pages 291–305, 2005.

[10] 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.

[11] Bertrand Jeannet and Antoine Miné. Apron: A library of numerical abstract domains for static analysis. In *Computer Aided Verification*, pages 661–667. Springer, 2009.

[12] Alex A Kurzhanskiy and Pravin Varaiya. Ellipsoidal toolbox (et). In *Decision and Control, 2006 45th IEEE Conference on*, pages 1498–1503. IEEE, 2006.

[13] Michal Kvasnica, Pascal Grieder, Mato Baotic, and Manfred Morari. Multi-parametric toolbox (mpt). In *HSCC*, pages 448–462. Springer, 2004.

[14] Gerardo Lafferriere, George J Pappas, and Sergio Yovine. *Decidable hybrid systems*. Citeseer, 1998.

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

[16] 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.

[17] Sriram Sankaranarayanan, Thao Dang, and Franjo Ivancic. Symbolic model checking of hybrid systems using template polyhedra. In *TACAS*, volume 4963 of *Lecture Notes in Computer Science*, pages 188–202. Springer-Verlag, 2008.

[18] Joseph K Scott, Davide M Raimondo, Giuseppe Roberto Marseglia, and Richard D Braatz. Constrained zonotopes: A new tool for set-based estimation and fault detection. *Automatica*, 69:126–136, 2016.