EPiC Series in Computer Science

Volume 34, 2015, Pages 120–151

ARCH14-15. 1st and 2nd International Workshop on Applied veRification for Continuous and Hybrid Systems

An Introduction to CORA 2015 (Tool Presentation)

Matthias Althoff

Technische Universität München, 85748 Garching, Germany
althoff@in.tum.de

Abstract

The philosophy, architecture, and capabilities of the COntinuous Reachability Analyzer (CORA) are presented. CORA is a toolbox that integrates various vector and matrix set representations and operations on them as well as reachability algorithms of various dynamic system classes. The software is designed such that set representations can be exchanged without having to modify the code for reachability analysis. CORA has a modular design, making it possible to use the capabilities of the various set representations for other purposes besides reachability analysis. The toolbox is designed using the object oriented paradigm, such that users can safely use methods without concerning themselves with detailed information hidden inside the object. Since the toolbox is written in MATLAB, the installation and use is platform independent.

Contents

1 Philosophy and Architecture

The **CO**ntinuous **R**eachability **A**nalyzer (CORA)[1] is a MATLAB toolbox for prototype design of algorithms for reachability analysis. The toolbox is designed for various kinds of systems with purely continuous dynamics (linear systems, nonlinear systems, differential-algebraic systems, parameter-varying systems, etc.) and hybrid dynamics combining the aforementioned continuous dynamics with discrete dynamics. Let us denote the continuous part of the solution of a hybrid system for a given initial discrete state by $\chi(t; x_0, u(\cdot), p)$, where $t \in \mathbb{R}$ is the time, $x_0 \in \mathbb{R}^n$ is the continuous initial state, $u(t) \in \mathbb{R}^m$ is the system input at t, $u(\cdot)$ is the input trajectory, and $p \in \mathbb{R}^p$ is a parameter vector. The continuous reachable set at time $t = r$ can be defined for a set of initial states $\mathcal{X}_0$, a set of input values $\mathcal{U}(t)$, and a set of parameter values $\mathcal{P}$, as

$$\mathcal{R}^e(r) = \Big\{ \chi(r; x_0, u(\cdot), p) \in \mathbb{R}^n \big| x_0 \in \mathcal{X}_0, \forall t : u(t) \in \mathcal{U}(t), p \in \mathcal{P} \Big\}.$$

CORA solely supports over-approximative computation of reachable sets since (a) exact reachable sets cannot be computed for most system classes [42] and (b) over-approximative computations qualify for formal verification. Thus, CORA computes over-approximations for particular points in time $\mathcal{R}(t) \supseteq \mathcal{R}^e(t)$ and for time intervals: $\mathcal{R}([t_0, t_f]) = \bigcup_{t \in [t_0, t_f]} \mathcal{R}(t)$.

CORA is built with the aim to construct one's own reachable set computation in a short amount of time. This is achieved by the following design choices:

- CORA is built for MATLAB, which is a script-based programming environment. Since the code does not have to be compiled, one can stop the program at any time and directly see the current values of variables. This makes it especially easy to understand the workings of the code and to debug new code.

[1] https://www6.in.tum.de/Main/SoftwareCORA

- CORA is an object-oriented toolbox that uses modularity, operator overloading, inheritance, and information hiding. One can safely use existing classes and just adapt classes one is interested in without redesigning the whole code. Operator overloading makes it possible to write formulas that look almost identical to the ones derived in scientific papers and thus reduce programming errors. Most of the information for each class is hidden and is not relevant to users of the toolbox. Most classes use identical methods so that set representations and dynamic systems can be effortlessly replaced.
- CORA interfaces with the established toolboxes MPTtoolbox[2] and INTLAB[3], which are also written in MATLAB. Results of CORA can be easily transferred to those toolboxes and vice versa.

1.1 Related Tools

Over the last years, many tools for formal verification of hybrid systems and for handling of continuous set representations have been developed. The following list of related tools is without any order; it is intended that related tools are grouped together. Tools based on, or supporting reachability analysis are *SpaceEx*, *Ellipsoidal Toolbox*, *Flow**, *COSY*, *VNODE-LP*, *A Toolbox of Level Set Methods*, and *Ariadne*. Tools based on constraint solving are *dReach*, *HySAT*, and *HSolver*. *KeYmaera* is an interactive theorem prover for verifying hybrid systems.

SpaceEx *SpaceEx*[4] [26] is the successor of *PHAVer* [25] for the computation of reachable sets of continuous and hybrid systems. *PHAVer* mainly focuses on hybrid systems with piecewise constant bounds on the derivatives. Linear continuous dynamics have to be abstracted by regions of constant bounds on the derivatives in *PHAVer*, resulting in scalability issues due to a large number of required regions. This problem is completely solved in *SpaceEx* by making use of a wrapping-free algorithm for linear continuous systems [33]. *SpaceEx* uses support functions as its main set representation, which scale very well for hybrid systems with linear continuous dynamics [27, 32]. *SpaceEx* computes reachable sets by computing successor sets of the reachable set for consecutive time intervals. The same basic approach is used in CORA.

SpaceEx does not only have a powerful analysis core, but is also easy to use due to a web-based graphical user interface and a graphical model editor. The model editor and its underlying language make it possible to construct complex models from simple components.

Ellipsoidal Toolbox The *Ellipsoidal Toolbox*[5] [41] is a MATLAB toolbox like CORA, but with a focus on ellipsoids as a set representation rather than zonotopes. Another difference is that different algorithms are used to compute abstractions of the system dynamics. Similarly to CORA, the toolbox supports a number of operations, such as Minkowski sum (under and over-approximation), intersection of ellipsoids with other set types, projections of ellipsoids, etc.

[2] http://people.ee.ethz.ch/~mpt/3/
[3] http://www.ti3.tu-harburg.de/rump/intlab/
[4] http://spaceex.imag.fr/
[5] http://systemanalysisdpt-cmc-msu.github.io/ellipsoids/

Flow* *Flow**[6] [21] also computes reachable sets of continuous and hybrid systems. It uses Taylor models to represent reachable sets, which can represent non-convex sets and are especially promising for reachability analysis of nonlinear models [17]. Instead of abstracting the dynamics on the level of the differential equation as done by *SpaceEx* and CORA, the abstraction is performed on the level of the solution of the differential equation. This can for instance be done using Picard iteration or truncated Lie series [22].

COSY *COSY*[7] is a tool for the rigorous computation of Taylor models, which are also used in *Flow**. *COSY* can be used to compute reachable sets of nonlinear differential-algebraic equations [37]. It is also useful to bound arbitrary nonlinear and multivariate functions by Taylor models [17].

VNODE-LP *VNODE-LP*[8] is a tool for guaranteed integration of ordinary differential equations. The focus of this tool is more on guaranteeing bounds of a single trajectory rather than computing reachable sets for safety verification. The tool computes reachable sets represented by boxes. A distinctive feature of the present solver is that it is developed entirely using literate programming [45].

A Toolbox of Level Set Methods *A Toolbox of Level Set Methods*[9] [43] computes approximations of the time-dependent Hamilton-Jacobi (HJ) partial differential equation (PDE). Since reachability problems can be reformulated as HJ PDEs [44], the toolbox computes approximations of reachable sets. The HJ PDEs are numerically solved by gridding the state space so that one can tune the accuracy of the result by varying the number of grid points. An advantage of this technique is that arbitrary non-convex sets can be handled. However, the approach has exponential complexity in the number of continuous state variables due to the exponential growth of grid points.

Ariadne *Ariadne*[10] [14] is a framework for hybrid automata verification. It differs from existing packages since it is based on the theory of computable analysis and on a rigorous function calculus. Extensions for assume-guaranteed verification are presented in [15].

dReach *dReach*[11] [29] is a tool for the safety verification of hybrid systems with nonlinear continuous dynamics. The tool is based on the SMT solver *dReal*[12] [28] for nonlinear theories over the reals. The basic idea is to reformulate ordinary differential equations as a set of constraints that are solved by the proposed SMT solver.

[6] http://systems.cs.colorado.edu/research/cyberphysical/taylormodels/
[7] http://www.bt.pa.msu.edu/index_cosy.htm
[8] http://www.cas.mcmaster.ca/~nedialk/vnodelp/
[9] http://www.cs.ubc.ca/~mitchell/ToolboxLS/index.html
[10] http://trac.parades.rm.cnr.it/ariadne/
[11] http://dreal.github.io/dReach/
[12] http://dreal.github.io/

HySAT Similarly to *dReach*, *HySAT*[13] [24] is a satisfiability checker for Boolean combinations of arithmetic constraints over real and integer-valued variables. It is the core for constraint-based verification for hybrid systems.

HSolver *HSolver*[14] [48] is designed for the safety verification of hybrid systems with nonlinear continuous dynamics. Similarly to *dReach*, *HSolver* constructs constraints from the system dynamics. The tool partitions the state space into a rectangular grid and applies interval arithmetic to compute which cells in the grid can be entered by a valid trajectory. The constraints are solved by pruning techniques.

KeYmaera *KeYmaera*[15] [47] is an interactive theorem prover for hybrid systems. *KeYmaera* supports *differential dynamic logic* (dL), which is a first-order dynamic logic for *hybrid programs* [46]. *Hybrid programs* are a different formalism for hybrid systems that are particularly suitable for logic-based verification.

Pioneering Tools Many of the aforementioned tools benefited from pioneering tools, which are no longer strongly supported: *HyTech*[16] [35], *HyperTech* [36], *d/dt* [11], *Checkmate*[17] [23], *VeriShift* [19], and *VERDICT* [40].

Tools for Timed Automata There also exist dedicated tools for the verification of timed automata, i.e. hybrid systems whose continuous state variables all have the dynamics $\dot{x}_i = 1$: UPPAL[18] [13], Kronos/Open-Kronoshttp:[19] [50], and STeP[20] [18]. While UPPAL is still maintained, the development of the other mentioned tools for timed automata seems to have stopped.

1.2 Architecture

The architecture of CORA can essentially be grouped into the following parts based on a separation of concerns as presented in Fig. 1 using UML[21]: Classes for set representations (Sec. 2), classes for matrix set representations (Sec. 3), classes for the analysis of continuous dynamics (Sec. 4), classes for the analysis of hybrid dynamics (Sec. 5), and a class for the partitioning of the state space (Sec. 6).

The class diagram in Fig. 1 shows that hybrid systems (class `hybridAutomaton`) consists of several instances of the `location` class. Each `location` object has a continuous dynamics (classes inheriting from `contDynamics`), several transitions (class `transition`), and a set representation (classes inheriting from `contSet`) to describe the invariant of the location. Each transition has

[13] http://www.uni-oldenburg.de/en/hysat/
[14] http://hsolver.sourceforge.net/
[15] http://symbolaris.com/info/KeYmaera.html
[16] http://embedded.eecs.berkeley.edu/research/hytech/
[17] http://www.mathworks.com/matlabcentral/fx_files/15441/3/content/doc/main.htm
[18] http://www.uppaal.org/
[19] http://www-verimag.imag.fr/~tripakis/openkronos.html
[20] http://www-step.stanford.edu/
[21] http://www.uml.org/

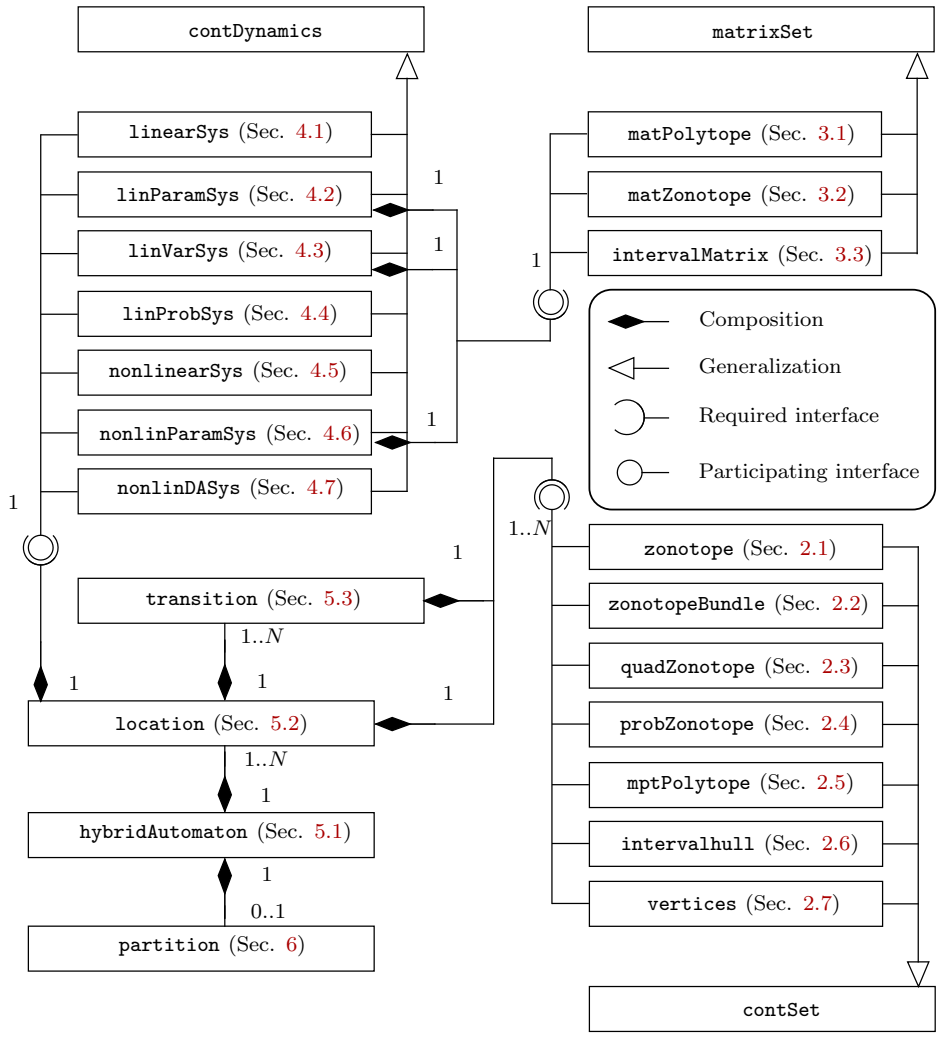


Figure 1: Unified Modeling Language (UML) class diagram of CORA 2015.

a set representation to describe the guard set enabling a transition to the next discrete state. More details on the semantics of those components can be found in Sec. 5.

Note that some classes subsume the functionality of other classes. For instance, nonlinear differential-algebraic systems (class `nonlinDASys`) are a generalization of nonlinear systems (class `nonlinearSys`). The reason why less general systems are not removed is because for those systems very efficient algorithms exist that are not applicable to more general systems.

2 Set Representations and Operations

The basis of any efficient reachability analysis is an appropriate set representation. On the one hand, the set representation should be general enough to describe the reachable sets accurately, on the other hand, it is crucial that the set representation makes it possible to run efficient and scalable operations on them. CORA provides a palette of set representations as depicted in Fig. 2, which also shows conversions supported between set representations.

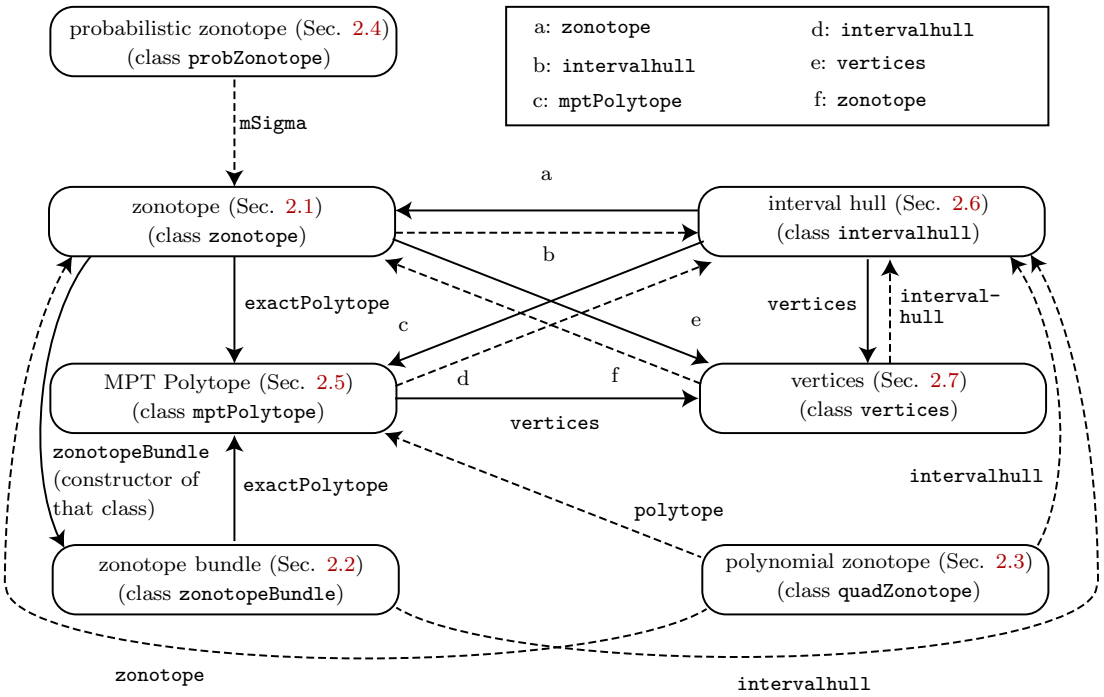


Figure 2: Set conversions supported. Solid arrows represent exact conversions, while dashed arrows represent over-approximative conversions. The arrows are labeled by the corresponding method to carry out the conversion.

Important operations for sets are:

- `display`: Displays the parameters of the set in the MATLAB workspace.
- `plot`: Plots a two-dimensional projection of a set in the current MATLAB figure.
- `mtimes`: Overloads the '`*`' operator for the multiplication of various objects with a set. For instance if M is a matrix of proper dimension and Z is a zonotope, `M * Z` returns the linear map $\{Mx|x \in Z\}$.
- `plus`: Overloads the '`+`' operator for the addition of various objects with a set. For instance if $Z1$ and $Z2$ are zonotopes of proper dimension, `Z1 + Z2` returns the Minkowsi sum $\{x + y|x \in Z1, y \in Z2\}$.
- `intervalhull`: Returns an interval hull that encloses the set (see Sec. 2.6).

2.1 Zonotopes

A zonotope is a geometric object in $\mathbb{R}^n$. Zonotopes are parameterized by a center $c \in \mathbb{R}^n$ and generators $g^{(i)} \in \mathbb{R}^n$ and defined as

$$\mathcal{Z} = \left\{ c + \sum_{i=1}^{p} \beta_i g^{(i)} \middle| \beta_i \in [-1, 1],\, c \in \mathbb{R}^n,\, g^{(i)} \in \mathbb{R}^n \right\}. \tag{1}$$

We write in short $\mathcal{Z} = (c, g^{(1)}, \ldots, g^{(p)})$. A zonotope can be interpreted as the Minkowski addition of line segments $l^{(i)} = [-1, 1]g^{(i)}$, and is visualized step-by-step in a two-dimensional vector space in Fig. 3. Zonotopes are a compact way of representing sets in high dimensions. More importantly, operations required for reachability analysis, such as linear maps $M \otimes \mathcal{Z} := \{Mz | z \in \mathcal{Z}\}$ ($M \in \mathbb{R}^{q \times n}$) and Minkowski addition $\mathcal{Z}_1 \oplus \mathcal{Z}_2 := \{z_1 + z_2 | z_1 \in \mathcal{Z}_1, z_2 \in \mathcal{Z}_2\}$ can be computed efficiently and exactly, and others such as convex hull computation can be tightly over-approximated [31]. The most important methods implemented are listed in Tab. 1.

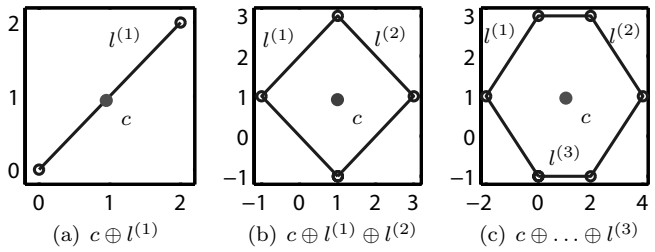


Figure 3: Step-by-step construction of a zonotope.

2.2 Zonotope Bundles

A disadvantage of zonotopes is that they are not closed under intersection, i.e., the intersection of two zonotopes does not return a zonotope in general. In order to overcome this disadvantage, zonotope bundles are introduced in [6]. Given a finite set of zonotopes $\mathcal{Z}_i$, a zonotope bundle is $\mathcal{Z}^{\cap} = \bigcap_{i=1}^{s} \mathcal{Z}_i$, i.e. the intersection of zonotopes $\mathcal{Z}_i$. Note that the intersection is not computed, but the zonotopes $\mathcal{Z}_i$ are stored in a list, which we write as $\mathcal{Z}^{\cap} = \{\mathcal{Z}_1, \ldots, \mathcal{Z}_s\}^{\cap}$. The most important methods implemented are listed in Tab. 2.

2.3 Polynomial Zonotopes

Zonotopes are a very efficient representation for reachability analysis of linear systems [31] and of nonlinear systems that can be well abstracted by linear differential inclusions [1]. However, more advanced techniques, such as in [2], abstract more accurately to nonlinear difference inclusions. As a consequence, linear maps of reachable sets are replaced by nonlinear maps. Zonotopes are not closed under nonlinear maps and are not particularly good at over-approximating them. For this reason, polynomial zonotopes are introduced in [2]. Polynomial zonotopes are a new non-convex set representation and can be efficiently stored and manipulated. The new

Table 1: Most important methods of the class `zonotope`.

name	description
`cartesianProduct`	returns the Cartesian product of two zonotopes.
`center`	returns the center of the zonotope.
`deleteZeros`	deletes generators whose entries are all zero.
`dim`	returns the dimension of a zonotope.
`display`	standard method (see Sec. 2).
`enclose`	generates a zonotope that encloses two zonotopes of equal dimension according to [1, Equation 2.2 + subsequent extension].
`enlarge`	enlarges the generators of a zonotope by a vector of factors for each dimension.
`exactPolytope`	returns an exact polytope in halfspace representation according to [1, Theorem 2.1].
`inParallelotope`	checks if a zonotope is a subset of a parallelotope, where the latter is represented as a zonotope.
`intervalhull`	standard method (see Sec. 2) according to [1, Proposition 2.2].
`mtimes`	standard method (see Sec. 2) for numeric matrices, `intval`/`intervalMatrix` according to [1, Theorem 3.3] and `matZonotope` according to [8, Sec. 4.4.1].
`plot`	standard method (see Sec. 2).
`plus`	standard method (see Sec. 2) for numeric vectors, and zonotopes according to [1, Equation 2.1].
`polytope`	returns an over-approximating polytope in halfspace representation according to heuristics in [1, Sec. 2.5.6.].
`project`	returns a zonotope, which is the projection of the input argument onto the specified dimensions.
`quadratic-Multiplication`	given a zonotope $\mathcal{Z}$ and a discrete set of matrices $Q^{(i)} \in \mathbb{R}^{n \times n}$ for $i = 1 \dots n$, `quadraticMultiplication` computes $\{\varphi \vert \varphi_i = x^T Q^{(i)} x, x \in \mathcal{Z}\}$ as described in [7, Lemma 1].
`randPoint`	generates a random point within a zonotope.
`reduce`	returns an over-approximating zonotope with fewer generators. Depending on the `options` struct, the reduction is performed according to [31, Sec. 3.4] or the methodology in [1, Section 2.5.5].
`split`	splits a zonotope into two or more zonotopes that enclose the original zonotope. Depending on the `options` struct, the split is performed as described in [1, Proposition 3.8] or [6, Section V.A].
`underapproximate`	returns the vertices of an under-approximation.
`vertices`	returns a `vertices` object including all vertices of the zonotope.
`volume`	computes the volume of a zonotope according to [34, p.40].
`zonotope`	constructor of the class.

representation shares many similarities with Taylor models [38] (as briefly discussed later) and is a generalization of zonotopes.

Given a *starting point* $c \in \mathbb{R}^n$, multi-indexed *generators* $f^{([i],j,k,\dots,m)} \in \mathbb{R}^n$, and single-indexed *generators* $g^{(i)} \in \mathbb{R}^n$, a polynomial zonotope is defined as

$$\mathcal{PZ} = \Big\{ c + \sum_{j=1}^{p} \beta_j f^{([1],j)} + \sum_{j=1}^{p} \sum_{k=j}^{p} \beta_j \beta_k f^{([2],j,k)} + \dots + \sum_{j=1}^{p} \sum_{k=j}^{p} \dots \sum_{m=l}^{p} \underbrace{\beta_j \beta_k \dots \beta_m}_{\eta \text{ factors}} f^{([\eta],j,k,\dots,m)} + \sum_{i=1}^{q} \gamma_i g^{(i)} \Big| \beta_i, \gamma_i \in [-1, 1] \Big\}. \tag{2}$$

The scalars β_i are called *dependent factors*, since changing their values does not only affect the multiplication with one generator, but with other generators too. On the other hand, the scalars γ_i only affect the multiplication with one generator, so they are called *independent factors*. The number of dependent factors is p, the number of independent factors is q, and the polynomial order η is the maximum power of the scalar factors β_i. The order of a polynomial zonotope is

Table 2: Most important methods of the class `zonotopeBundle`.

name	description
`and`	returns the intersection with a zonotope bundle or a zonotope.
`display`	standard method (see Sec. 2).
`enclose`	generates a zonotope bundle that encloses two zonotope bundles of equal dimension according to [6, Proposition 5].
`encloseTight`	generates a zonotope bundle that encloses two zonotope bundles in a possibly tighter way than `enclose` as outlined in [6, Sec. VI.A].
`enlarge`	enlarges the generators of each zonotope in the bundle by a vector of factors.
`exactPolytope`	returns an exact polytope in halfspace representation by applying [1, Theorem 2.1] to each zonotope.
`intervalhull`	standard method (see Sec. 2) according to [6, Proposition 6].
`mtimes`	standard method (Sec. 2) according to [6, Proposition 1].
`plot`	standard method (Sec. 2).
`plus`	standard method (see Sec. 2) according to [6, Proposition 2].
`polytope`	returns an over-approximating polytope in halfspace representation.
`project`	returns a zonotope bundle, which is the projection of the input argument onto the specified dimensions.
`reduce`	returns an over-approximating zonotope bundle with less generators.
`reduceCombined`	reduces the order of a zonotope bundle, not by reducing each zonotope separately as in `reduce`, but in a combined fashion.
`shrink`	shrinks the size of individual zonotopes by explicitly computing the intersection of individual zonotopes.
`split`	splits a zonotope bundle into two or more zonotopes bundles. In contrast to the function for zonotopes, the split is exact.
`volume`	computes the volume of a zonotope bundle.
`zonotopeBundle`	constructor of the class.

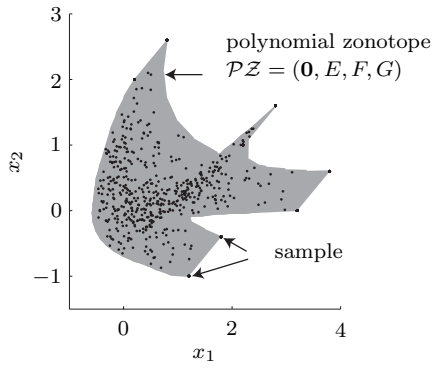
defined as the number of generators ξ divided by the dimension, which is $\rho = \frac{\xi}{n}$. For a concise notation and later derivations, we introduce the matrices

$$
\begin{aligned}
E^{[i]} &= [\underbrace{f^{([i],1,1,\ldots,1)}}_{=:e^{([i],1)}} \ldots \underbrace{f^{([i],p,p,\ldots,p)}}_{=:e^{([i],p)}}] \text{ (all indices are the same value)},\\
F^{[i]} &= [f^{([i],1,1,\ldots,1,2)}\ f^{([i],1,1,\ldots,1,3)} \ \ldots\ f^{([i],1,1,\ldots,1,p)}\\
&\quad\ f^{([i],1,1,\ldots,2,2)}\ f^{([i],1,1,\ldots,2,3)} \ \ldots\ f^{([i],1,1,\ldots,2,p)}\\
&\quad\ f^{([i],1,1,\ldots,3,3)} \ldots] \text{ (not all indices are the same value)},\\
G &= [g^{(1)} \ \ldots\ g^{(q)}],
\end{aligned}
$$

and $E = \begin{bmatrix} E^{[1]} & \ldots & E^{[\eta]} \end{bmatrix}$, $F = \begin{bmatrix} F^{[2]} & \ldots & F^{[\eta]} \end{bmatrix}$ ($F^{[i]}$ is only defined for $i \geq 2$). Note that the indices in $F^{[i]}$ are ascending due to the nested summations in (2). In short form, a polynomial zonotope is written as $\mathcal{PZ} = (c, E, F, G)$.

For a given polynomial order i, the total number of generators in $E^{[i]}$ and $F^{[i]}$ is derived using the number $\binom{p+i-1}{i}$ of combinations of the scalar factors β with replacement (i.e. the same factor can be used again). Adding the numbers for all polynomial orders and adding the number of independent generators q, results in $\xi = \sum_{i=1}^{\eta} \binom{p+i-1}{i} + q$ generators, which is in $\mathcal{O}(p^\eta)$ with respect to p. The non-convex shape of a polynomial zonotope with polynomial order 2 is shown in Fig. 4.

So far, polynomial zonotopes are only implemented up to polynomial order $\eta = 2$ so that the subsequent class is called `quadZonotope` due to the quadratic polynomial order. The most important methods implemented are listed in Tab. 3.



$$E^{[1]} = \begin{bmatrix} -1 & 0 \\ 0 & 0.5 \end{bmatrix}$$
$$E^{[2]} = \begin{bmatrix} 1 & 1 \\ 0.5 & 0.3 \end{bmatrix}$$
$$F^{[2]} = \begin{bmatrix} -0.5 \\ 1 \end{bmatrix}$$
$$G = \begin{bmatrix} 0.3 \\ 0.3 \end{bmatrix}$$

Figure 4: Over-approximative plot of a polynomial zonotope as specified in the figure. Random samples of possible values demonstrate the accuracy of the over-approximative plot.

Table 3: Most important methods of the class `quadZonotope`.

name	**description**
`cartesianProduct`	returns the Cartesian product of a `quadZonotope` and a `zonotope`.
`center`	returns the starting point c.
`display`	standard method (see Sec. 2).
`enclose`	generates an over-approximative `quadZonotope` that encloses two `quadZonotopes`.
`generators`	returns the generators of a `quadZonotope`.
`intervalhull`	standard method (see Sec. 2). Other than for the `zonotope` class, the generated interval hull is not tight in the sense that it touches the `quadZonotope`.
`intervalhull-Accurate`	over-approximates a `quadZonotope` by a tighter interval hull as when applying `intervalhull`.
`mtimes`	standard method (see Sec. 2) as stated in [6, Equation 14] for numeric matrix multiplication and as described in [1, Theorem 3.3] for interval matrices.
`plot`	standard method (see Sec. 2).
`plus`	standard method (see Sec. 2) for numeric vectors, `zonotope` objects, and `quadZonotope` objects.
`pointSet`	computes a user-defined number of random points within the `quadZonotope`.
`pointSetExtreme`	computes a user-defined number of random points when only allowing the values $\{-1, 1\}$ for β_i, γ_i (see (2)).
`polytope`	returns an over-approximating polytope in halfspace representation.
`project`	returns a `quadZonotope`, which is the projection of the input argument onto the specified dimensions.
`quadratic-Multiplication`	given a `quadZonotope` $\mathcal{Z}$ and a discrete set of matrices $Q^{(i)} \in \mathbb{R}^{n \times n}$ for $i = 1 \dots n$, `quadraticMultiplication` computes $\{\varphi | \varphi_i = x^T Q^{(i)} x, x \in \mathcal{Z}\}$ as described in [2, Corollary 1].
`quadZonotope`	constructor of the class.
`randPoint`	computes a random point within the `quadZonotope`.
`randPointExtreme`	computes a random point when only allowing the values $\{-1, 1\}$ for β_i, γ_i (see (2)).
`reduce`	returns an over-approximating `quadZonotope` with fewer generators. The redistribution technique is according to [2, Proposition 2] and the standard technique according to [31, Sec. 3.4].
`splitLongestGen`	splits the longest generator factor and returns two `quadZonotope` objects.
`splitOneGen`	splits one generator factor and returns two `quadZonotope` objects.
`zonotope`	computes an enclosing zonotope as presented in [2, Proposition 1].

2.4 Probabilistic Zonotopes

Probabilistic zonotopes have been introduced in [10] for stochastic verification. A probabilistic zonotope has the same structure as a zonotope, except that the values of some β_i in (1) are

bounded by the interval $[-1, 1]$, while others are subject to a normal distribution [22]. Given pairwise independent Gaussian distributed random variables $\mathcal{N}(\mu, \Sigma)$ with expected value μ and covariance matrix Σ, one can define a Gaussian zonotope with certain mean:

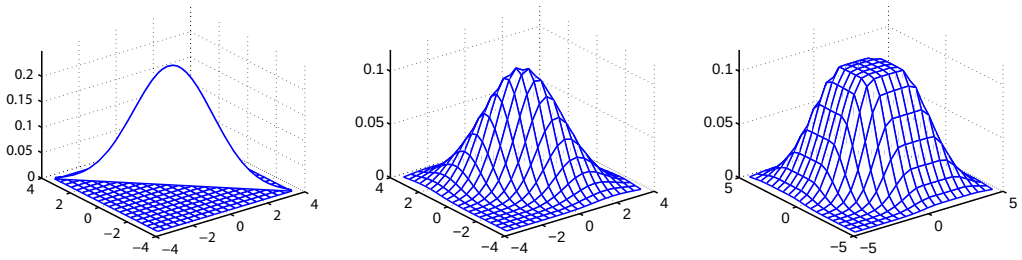
$$\mathcal{Z}_g = c + \sum_{i=1}^{q} \mathcal{N}^{(i)}(0, 1) \cdot \underline{g}^{(i)},$$

where $\underline{g}^{(1)}, \ldots, \underline{g}^{(q)} \in \mathbb{R}^n$ are the generators, which are underlined in order to distinguish them from generators of regular zonotopes. Gaussian zonotopes are denoted by a subscripted g: $\mathcal{Z}_g = (c, \underline{g}^{(1\ldots q)})$.

A Gaussian zonotope with uncertain mean $\mathscr{Z}$ is defined as a Gaussian zonotope $\mathcal{Z}_g$, where the center is uncertain and can have any value within a zonotope $\mathcal{Z}$, which is denoted by

$$\mathscr{Z} := \mathcal{Z} \boxplus \mathcal{Z}_g, \quad \mathcal{Z} = (c, g^{(1\ldots p)}),\ \mathcal{Z}_g = (0, \underline{g}^{(1\ldots q)}).$$

or in short by $\mathscr{Z} = (c, g^{(1\ldots p)}, \underline{g}^{(1\ldots q)})$. If the probabilistic generators can be represented by the covariance matrix Σ ($q > n$) as shown in [10, Proposition 1], one can also write $\mathscr{Z} = (c, g^{(1\ldots p)}, \Sigma)$. As $\mathscr{Z}$ is neither a set nor a random vector, there does not exist a probability density function describing $\mathscr{Z}$. However, one can obtain an enclosing probabilistic hull which is defined as $\bar{f}_{\mathscr{Z}}(x) = \sup\left\{ f_{\mathcal{Z}_g}(x) \middle| E[\mathcal{Z}_g] \in Z \right\}$, where $E[\,]$ returns the expectation and $f_{\mathcal{Z}_g}(x)$ is the probability density function (PDF) of $\mathcal{Z}_g$. Combinations of sets with random vectors have also been investigated, e.g. in [16]. Analogously to a zonotope, it is shown in Fig. 5 how the enclosing probabilistic hull (EPH) of a Gaussian zonotope with two non-probabilistic and two probabilistic generators is built step-by-step from left to right. The most important methods implemented are listed in Tab. 4.



(a) PDF of $(0, \underline{g}^{(1)})$. (b) PDF of $(0, \underline{g}^{(1,2)})$. (c) EPH of $(0, g^{(1\ldots 2)}, \underline{g}^{(1\ldots 2)})$.

Figure 5: Construction of a probabilistic zonotope.

2.5 MPT Polytopes

There exist two representations for polytopes: The halfspace representation (H-representation) and the vertex representation (V-representation). The halfspace representation specifies a convex polytope $\mathcal{P}$ by the intersection of q halfspaces $\mathcal{H}^{(i)}$: $\mathcal{P} = \mathcal{H}^{(1)} \cap \mathcal{H}^{(i)} \cap \ldots \cap \mathcal{H}^{(q)}$. A

[22] Other distributions are conceivable, but not implemented.

Table 4: Most important methods of the class `probZonotope`.

name	description
`center`	returns the center of the probabilistic zonotope.
`display`	standard method (see Sec. 2).
`enclose`	generates a probabilistic zonotope that encloses two probabilistic zonotopes $\mathcal{Z}$, $A \otimes \mathcal{Z}$ ($A \in \mathbb{R}^{n \times n}$) according to [10, Section VI.A].
`enclosing-Probability`	computes values to plot the mesh of a two-dimensional projection of the enclosing probability hull.
`max`	computes an over-approximation of the maximum on the m-sigma bound according to [10, Equation 3].
`mean`	returns the uncertain mean of a probabilistic zonotope.
`mSigma`	converts a probabilistic zonotope to a common zonotope where for each generator, an m-sigma interval is taken.
`mtimes`	standard method (see Sec. 2) as stated in [10, Equation 4] for numeric matrix multiplication. The multiplication of interval matrices is also supported.
`plot`	standard method (see Sec. 2).
`plus`	standard method (see Sec. 2) for numeric vectors, `zonotope` objects, and `probZonotope` objects as described in [10, Equation 4].
`probReduce`	reduces the number of single Gaussian distributions to the dimension of the state space.
`probZonotope`	constructor of the class.
`pyramid`	implementation of [10, Section VI.C] to obtain the probability of intersecting a polytope.
`reduce`	returns an over-approximating zonotope with fewer generators.
`sigma`	returns the Σ matrix of a probabilistic zonotope.

halfspace is one of the two parts obtained by bisecting the n-dimensional Euclidean space with a hyperplane $\mathcal{S}$, which is given by $\mathcal{S} := \{x | c^T x = d\}, c \in \mathbb{R}^n, d \in \mathbb{R}$. The vector c is the normal vector of the hyperplane and d the scalar product of any point on the hyperplane with the normal vector. From this follows that the corresponding halfspace is $\mathcal{H} := \{x | c^T x \leq d\}$. As the convex polytope $\mathcal{P}$ is the nonempty intersection of q halfspaces, q inequalities have to be fulfilled simultaneously.

H-Representation of a Polytope A convex polytope $\mathcal{P}$ is the bounded intersection of q halfspaces:

$$\mathcal{P} = \left\{ x \in \mathbb{R}^n \middle| C\,x \leq d, \quad C \in \mathbb{R}^{q \times n}, d \in \mathbb{R}^q \right\}.$$

When the intersection is unbounded, one obtains a polyhedron [52].

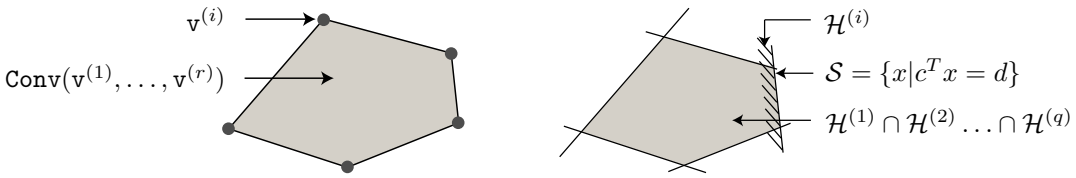
A polytope with vertex representation is defined as the convex hull of a finite set of points in the n-dimensional Euclidean space. The points are also referred to as vertices and are denoted by $\mathtt{v}^{(i)} \in \mathbb{R}^n$. A convex hull of a finite set of r points is obtained from their linear combination:

$$\mathtt{Conv}(\mathtt{v}^{(1)}, \ldots, \mathtt{v}^{(r)}) := \left\{ \sum_{i=1}^{r} \alpha_i \mathtt{v}^{(i)} \middle| \mathtt{v}^{(i)} \in \mathbb{R}^n,\, \alpha_i \in \mathbb{R},\, \alpha_i \geq 0,\, \sum_{i=1}^{r} \alpha_i = 1 \right\}.$$

Given the convex hull operator `Conv()`, a convex and bounded polytope can be defined in vertex representation as follows:

V-Representation of a Polytope For r vertices $\mathtt{v}^{(i)} \in \mathbb{R}^n$, a convex polytope $\mathcal{P}$ is the set $\mathcal{P} = \mathtt{Conv}(\mathtt{v}^{(1)}, \ldots, \mathtt{v}^{(r)})$.

The halfspace and the vertex representation are illustrated in Fig. 6. Algorithms that convert from H- to V-representation and vice versa are presented in [39].



(a) $V-representation$ (b) $H-representation$

Figure 6: Possible representations of a polytope.

The class `mptPolytope` is a wrapper class that interfaces with the MATLAB toolbox *Multi-Parametric Toolbox* (MPT) for the methods listed in Tab. 5.

Table 5: Most important methods of the class `mptPolytope`.

name	description
`and`	computes the intersection of two `mptPolytopes`.
`display`	standard method (see Sec. 2).
`enclose`	computes the convex hull of two `mptPolytopes`.
`in`	determines if a `zonotope` is enclosed by a `mptPolytope`.
`interval`	encloses a `mptPolytope` by INTLAB intervals.
`intervalhull`	encloses a `mptPolytope` by an `intervalhull`.
`iscontained`	returns if a `mptPolytope` is contained in another `mptPolytope`.
`is_empty`	returns 1 if a `mptPolytope` is empty and 0 otherwise.
`mldivide`	computes the set difference of two `mptPolytopes`.
`mptPolytope`	constructor of the class.
`mtimes`	standard method (see Sec. 2) for numeric and interval matrix multiplication.
`plot`	standard method (see Sec. 2).
`plus`	standard method (see Sec. 2) for numeric vectors and `mptPolytope` objects.
`vertices`	returns a `vertices` object including all vertices of the polytope.
`volume`	computes the volume of a polytope.

2.6 Interval Hulls

An interval hull $\mathcal{I}$ is the closest axis-aligned box of a set. It can easily be represented as a multidimensional interval: $\mathcal{I} = [\underline{x}, \overline{x}]$, $\underline{x} \in \mathbb{R}^n$, $\overline{x} \in \mathbb{R}^n$, $\forall i : \underline{x}_i \leq \overline{x}_i$. We provide the methods in Tab. 6.

2.7 Vertices

The `vertices` class has two main purposes: It is the class that performs the plotting since all other set representations are first converted to vertices to perform the plotting. Second, if one defines a point cloud as a set of potential vertices, this class computes enclosures of all points. The methods are listed in Tab. 7.

Table 6: Most important methods of the class `intervalhull`.

name	description
`abs`	returns the absolute value bound of an interval hull: $\lvert\mathcal{I}\rvert_i = \sup\{\lvert x_i\rvert \mid x \in \mathcal{I}\}$.
`and`	computes the intersection of two `intervalhulls`.
`center`	returns the center of the `intervalhull`.
`display`	standard method (see Sec. 2).
`edgeLength`	determines the edge lengths of the interval hull.
`enclose`	computes an interval hull that encloses two interval hulls.
`halfspace`	generates halfspace representation of the `intervalhull`.
`in`	determines if a `zonotope` is enclosed by the `intervalhull`.
`inf`	returns the infimum of an intervalhull.
`interval`	converts an `intervalhull` to INTLAB intervals.
`intervalhull`	constructor of the class.
`is_empty`	returns 1 if a `intervalhull` is empty and 0 otherwise.
`le`	overloads `<=` operator: Is one interval hull equal or the subset of another interval hull?
`lt`	overloads `<` operator: Is one interval hull equal or the subset of another interval hull?
`mptPolytope`	converts an `intervalhull` object to a `mptPolytope` object.
`mtimes`	standard method (see Sec. 2) for numeric and interval matrix multiplication.
`or`	over-approximates the union of interval hulls.
`plot`	standard method (see Sec. 2).
`plus`	standard method (see Sec. 2) for numeric vectors and `intervalhull` objects.
`polytope`	converts an interval hull object to a polytope.
`radius`	computes radius of an enclosing circle.
`rdivide`	overloads the `./` operator; elementwise division of intervals by a vector.
`sup`	returns the supremum of an intervalhull.
`vertices`	returns a `vertices` object including all vertices.
`volume`	computes the volume of an interval hull.
`zonotope`	converts an `intervalhull` object to a `zonotope` object.

Table 7: Most important methods of the class `vertices`.

name	description
`collect`	collects cell arrays (MATLAB-specific container) of vertices.
`display`	standard method (see Sec. 2).
`intervalhull`	encloses all vertices by an `intervalhull`.
`mtimes`	standard method (see Sec. 2) for numeric matrix multiplication.
`parallelotope`	computes a enclosing parallelotope for provided facet normals.
`plot`	standard method (see Sec. 2).
`plus`	standard method (see Sec. 2) for nuemric vectors.
`vertices`	constructor of the class.
`zonotope`	computes a zonotope that encloses all vertices according to [49, Section 3].

3 Matrix Set Representations and Operations

Besides vector sets as introduced in the previous section, it is often useful to represent sets of possible matrices. This occurs for instance, when a linear system has uncertain parameters as described later in Sec. 4.2. CORA supports the following matrix set representations:

- Matrix polytope (Sec. 3.1)
- Matrix zonotope (Sec. 3.2); specialization of a matrix polytope.
- Interval matrix (Sec. 3.3); specialization of a matrix zonotope.

For each matrix set representation, the conversion to all other matrix set computations is implemented. Of course, conversions to specializations are realized in an over-approximative

way, while the other direction is computed exactly. Note that we use the term *matrix polytope* instead of *polytope matrix*. The reason is that the analogous term *vector polytope* makes sense, while *polytope vector* can be misinterpreted as a vertex of a polytope. We do not use the term *matrix interval* since the term *interval matrix* is already established. Important operations for matrix sets are

- `display`: Displays the parameters of the set in the MATLAB workspace.
- `mtimes`: Overloads the '`*`' operator for the multiplication of various objects with a matrix set. For instance if M_set is a matrix set of proper dimension and Z is a zonotope, `M_set * Z` returns the linear map $\{Mx|M \in M\_set, x \in Z\}$.
- `plus`: Overloads the '`+`' operator for the addition of various objects with a matrix set. For instance if $M1\_set$ and $M2\_set$ are interval matrices of proper dimension, `M1_set + M2_set` returns the Minkowski sum $\{M1 + M2|M1 \in M1\_set, M2 \in M2\_set\}$.
- `expm`: Returns the set of matrix exponentials for a matrix set.
- `intervalMatrix`: Computes an enclosing interval matrix.
- `vertices`: returns the vertices of a matrix set.

3.1 Matrix Polytopes

A matrix polytope is analogously defined as a V-polytope (see Sec. 2.5):

$$\mathcal{A}_{[p]} = \Big\{ \sum_{i=1}^{r} \alpha_i V^{(i)} \Big| V^{(i)} \in \mathbb{R}^{n \times n}, \alpha_i \in \mathbb{R}, \alpha_i \geq 0, \sum_i \alpha_i = 1 \Big\}. \tag{3}$$

The matrices $V^{(i)}$ are also called vertices of the matrix polytope. When substituting the matrix vertices by vector vertices $v^{(i)} \in \mathbb{R}^n$, one obtains a V-polytope (see Sec. 2.5). The methods in Tab. 8 are implemented.

Table 8: Most important methods of the class `matPolytope`.

name	description
`display`	standard method (see Sec. 3).
`expmInd`	operator for the exponential matrix of a matrix polytope, evaluated independently.
`expmIndMixed`	operator for the exponential matrix of a matrix polytope, evaluated independently. Higher order terms are computed using interval arithmetic.
`intervalMatrix`	standard method (see Sec. 3).
`matPolytope`	constructor of the class.
`matZonotope`	computes an enclosing matrix zonotope.
`mpower`	overloaded '^' operator for the power of matrix polytopes.
`mtimes`	standard method (see Sec. 3) for numeric matrix multiplication or multiplication with another matrix polytope.
`plot`	plots a 2-dimensional projection of a matrix polytope.
`powers`	computes the powers of a matrix zonotope up to a certain order.
`plus`	standard method (see Sec. 3) for a matrix polytope or a numeric matrix.
`polytope`	converts a matrix polytope to a polytope.
`simplePlus`	computes the Minkowski addition of two matrix polytopes.
`vertices`	standard method (see Sec. 3).

3.2 Matrix Zonotopes

A matrix zonotope is defined analogously to zonotopes (see Sec. 2.1):

$$\mathcal{A}_{[z]} = \left\{ G^{(0)} + \sum_{i=1}^{\kappa} p_i G^{(i)} \middle| p_i \in [-1,1], G^{(i)} \in \mathbb{R}^{n \times n} \right\} \tag{4}$$

and is written in short form as $\mathcal{A}_{[z]} = (G^{(0)}, G^{(1)}, \ldots, G^{(\kappa)})$, where the first matrix is referred to as the *matrix center* and the other matrices as *matrix generators*. The order of a matrix zonotope is defined as $\rho = \kappa/n$. When exchanging the matrix generators by vector generators $g^{(i)} \in \mathbb{R}^n$, one obtains a zonotope (see e.g. [31]). The methods for matrix zonotopes are listed in Tab. 9.

Table 9: Most important methods of the class `matZonotope`.

name	description
`concatenate`	concatenates the center and all generators of two matrix zonotopes.
`display`	standard method (see Sec. 3).
`dependentTerms`	considers dependency in the computation of Taylor terms for the matrix zonotope exponential according to [8, Proposition 4.3].
`dominantVertices`	computes the dominant vertices of a matrix zonotope according to a heuristics.
`expmInd`	operator for the exponential matrix of a matrix zonotope, evaluated independently.
`expmIndMixed`	operator for the exponential matrix of a matrix zonotope, evaluated independently. Higher order terms are computed using interval arithmetic.
`expmMixed`	operator for the exponential matrix of a matrix zonotope, evaluated dependently. Higher order terms are computed using interval arithmetic [8, Section 4.4.4].
`expmOneParam`	operator for the exponential matrix of a matrix zonotope when only one parameter is uncertain [4, Theorem 1].
`expmVertex`	computes the exponential matrix for a selected number of dominant vertices obtained by the `dominantVertices` method.
`infNorm`	returns the maximum of the infinity norm of a matrix zonotope.
`infNormRed`	returns a fast over-approximation of the maximum of the infinity norm of a matrix zonotope.
`intervalMatrix`	standard method (see Sec. 3).
`matPolytope`	converts a matrix zonotope into a matrix polytope representation.
`matZonotope`	constructor of the class.
`mpower`	overloaded '^' operator for the power of matrix zonotopes.
`mtimes`	standard method (see Sec. 3) for numeric matrix multiplication or multiplication with another matrix zonotope according to [8, Equation 4.10].
`plot`	plots 2-dimensional projection of a matrix zonotope.
`plus`	standard method (see Sec. 3) for a matrix zonotope or a numerical matrix.
`powers`	computes the powers of a matrix zonotope up to a certain order.
`reduce`	reduces the order of a matrix zonotope.
`uniformSampling`	creates samples uniformly within a matrix zonotope.
`vertices`	standard method (see Sec. 3).
`volume`	computes the volume of a matrix zonotope by computing the volume of the corresponding zonotope.
`zonotope`	converts a matrix zonotope into a zonotope.

3.3 Interval Matrices

An interval matrix is a special case of a matrix zonotope and specifies the interval of possible values for each matrix element:

$$\mathcal{A}_{[i]} = [\underline{A}, \overline{A}], \quad \forall i,j : \underline{a}_{ij} \leq \overline{a}_{ij}, \quad \underline{A}, \overline{A} \in \mathbb{R}^{n \times n}.$$

The matrix $\underline{A}$ is referred to as the *lower bound* and $\overline{A}$ as the *upper bound* of $\mathcal{A}_{[i]}$. The methods for interval matrices are listed in Tab. 10.

Table 10: Most important methods of the class `intervalMatrix`.

name	description
`abs`	returns the absolute value bound of an interval matrix.
`display`	standard method (see Sec. 3).
`dependentTerms`	considers dependency in the computation of Taylor terms for the interval matrix exponential according to [8, Proposition 4.4].
`dominantVertices`	computes the dominant vertices of an interval matrix zonotope according to a heuristics.
`expm`	operator for the exponential matrix of an interval matrix, evaluated dependently.
`expmAbsoluteBound`	returns the over-approximation of the absolute bound of the symmetric solution to the computation of the exponential matrix.
`expmInd`	operator for the exponential matrix of an interval matrix, evaluated independently.
`expmNormInf`	returns the over-approximation of the norm of the difference between the interval matrix exponential and the exponential from the center matrix according to [8, Theorem 4.2].
`expmVertex`	computes the exponential matrix for a selected number of dominant vertices obtained by the `dominantVertices` method.
`exponentialRemainder`	returns the remainder of the exponential matrix according to [8, Proposition 4.1].
`infNorm`	returns the maximum of the infinity norm of an interval matrix.
`intervalhull`	converts an interval matrix to an interval hull.
`intervalMatrix`	constructor of the class.
`matPolytope`	converts an interval matrix to a matrix polytope.
`matZonotope`	converts an interval matrix to a matrix zonotope.
`mpower`	overloaded '^' operator for the power of interval matrices.
`mtimes`	standard method (see Sec. 3) for numeric matrix multiplication or multiplication with another interval matrix according to [8, Equation 4.11].
`plot`	plots a 2-dimensional projection of an interval matrix.
`plus`	standard method (see Sec. 3) for another interval matrix or a numeric matrix.
`powers`	computes the powers of an interval matrix up to a certain order.
`randomIntervalMatrix`	generates a random interval matrix with a specified center and a specified delta matrix or scalar.
`uniformSampling`	creates samples uniformly within an interval matrix.
`vertices`	standard method (see Sec. 3).
`volume`	computes the volume of an interval matrix by computing the volume of the corresponding interval hull.

4 Continuous Dynamics

This section introduces various classes to compute reachable sets of continuous dynamics. One can directly compute reachable sets for each class, or include those classes into a hybrid automaton for the reachability analysis of hybrid systems. Note that besides reachability analysis, the simulation of particular trajectories is also supported. CORA supports the following continuous dynamics:

- Linear systems (Sec. 4.1)
- Linear systems with uncertain fixed parameters (Sec. 4.2)
- Linear systems with uncertain varying parameters (Sec. 4.3)
- Linear probabilistic systems (Sec. 4.4)
- Nonlinear systems (Sec. 4.5)

- Nonlinear systems with uncertain fixed parameters (Sec. 4.6)
- Nonlinear differential-algebraic systems (Sec. 4.7)

For each class the same methods are implemented:

- `display`: Displays the parameters of the continuous dynamics in the MATLAB workspace.
- `initReach`: Initializes the reachable set computation.
- `reach`: Computes the reachable set for the next time interval.
- `simulate`: Produces a single trajectory that numerically solves the system for a particular initial state and a particular input trajectory.

There exist some further auxiliary methods for each class, but those are not relevant unless one aims to change details of the provided algorithms. In contrast to the set representations, all continuous systems have the same methods, therefor the methods are not listed for the individual classes. We mainly focus on the method `initReach`, which is computed differently for each class.

4.1 Linear Systems

The most basic system dynamics considered in this software package are linear systems of the form

$$\dot{x}(t) = Ax(t) + Bu(t), \quad x(0) \in \mathcal{X}_O \subset \mathbb{R}^n, \quad u(t) \in \mathcal{U} \subset \mathbb{R}^n \tag{5}$$

For the computation of reachable sets, we use the equivalent system

$$\dot{x}(t) = Ax(t) + \tilde{u}(t), \quad x(0) \in \mathcal{X}_O \subset \mathbb{R}^n, \quad \tilde{u}(t) \in \tilde{\mathcal{U}} = B \otimes \mathcal{U} \subset \mathbb{R}^n, \tag{6}$$

where $\mathcal{C} \otimes \mathcal{D} = \{C\,D | C \in \mathcal{C}, D \in \mathcal{D}\}$ is the set-based multiplication (one argument can be a singleton).

The method `initReach` computes the required steps to obtain the reachable set for the first point in time r and the first time interval $[0, r]$ as follows. Given is the linear system in (6). For further computations, we introduce the center of the set of inputs u_c and the deviation from the center of $\tilde{\mathcal{U}}$, $\tilde{\mathcal{U}}_\Delta := \tilde{\mathcal{U}} \oplus (-u_c)$. According to [1, Section 3.2], the reachable set for the first time interval $\tau_0 = [0, r]$ is computed as shown in Fig. 7:

1. Starting from $\mathcal{X}_O$, compute the set of all solutions $\mathcal{R}_h^d$ for the affine dynamics $\dot{x}(t) = Ax(t) + u_c$ at time r.
2. Obtain the convex hull of $\mathcal{X}_O$ and $\mathcal{R}_h^d$ to approximate the reachable set for the first time interval τ_0.
3. Compute $\mathcal{R}^d(\tau_0)$ by enlarging the convex hull, firstly to bound all affine solutions within τ_0 and secondly to account for the set of uncertain inputs $\tilde{\mathcal{U}}_\Delta$.

4.2 Linear Systems with Uncertain Fixed Parameters

This class extends linear systems by uncertain parameters that are fixed over time:

$$\dot{x}(t) = A(p)x(t) + \tilde{u}(t), \quad x(0) \in \mathcal{X}_O \subset \mathbb{R}^n, \quad p \in \mathcal{P}, \quad \tilde{u}(t) \in \tilde{\mathcal{U}} = \{B(p) \otimes \mathcal{U} | \mathcal{U} \subset \mathbb{R}^n, p \in \mathcal{P}\}, \tag{7}$$

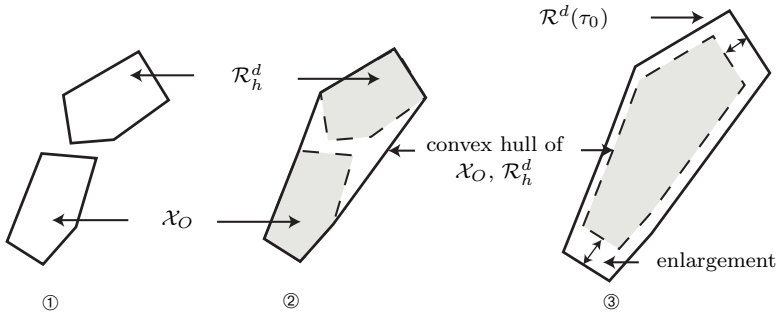


Figure 7: Steps for the computation of an over-approximation of the reachable set for a linear system.

The set of state and input matrices is denoted by

$$\mathcal{A} = \{A(p)|p \in \mathcal{P}\}, \quad \mathcal{B} = \{B(p)|p \in \mathcal{P}\} \tag{8}$$

An alternative is to define each parameter as a state variable $\tilde{x}_i$ with the trivial dynamics $\dot{\tilde{x}}_i = 0$. The result is a nonlinear system that can be handled as described in Sec. 4.5. The problem of which approach to use for any particular case is still open.

The method `initReach` computes the reachable set for the first point in time r and the first time interval $[0, r]$ similarly as for linear systems with fixed parameters. The main difference is that we have to take into account an uncertain state matrix $\mathcal{A}$ and an uncertain input matrix $\mathcal{B}$. The initial state solution becomes

$$\mathcal{R}_h^d = e^{\mathcal{A}r}\mathcal{X}_O = \{e^{Ar}x_0|A \in \mathcal{A}, x_0 \in \mathcal{X}_O\}. \tag{9}$$

Similarly, the reachable set due to the input solution changes as described in [1, Section 3.3].

4.3 Linear Systems with Uncertain Varying Parameters

This class extends linear systems with uncertain, but fixed parameters to linear systems with time-varying parameters:

$$\dot{x}(t) = A(t)x(t) + \tilde{u}(t), \quad x(0) \in \mathcal{X}_O \subset \mathbb{R}^n, \quad A(t) \in \mathcal{A}, \quad \tilde{u}(t) \in \tilde{\mathcal{U}}.$$

The set of state matrices can be represented by any matrix set introduced in Sec. 3. The provided methods of the class are identical to the ones in Sec. 4.2, except that the computation is based on [9].

4.4 Linear Probabilistic Systems

In contrast to all other systems, we consider stochastic properties in the class `linProbSys`. The system under consideration is defined by the following linear stochastic differential equation (SDE) which is also known as the multivariate Ornstein-Uhlenbeck process [30]:

$$\begin{aligned} \dot{x} &= Ax(t) + u(t) + C\xi(t), \\ x(0) \in \mathbb{R}^n,\ u(t) &\in \mathcal{U} \subset \mathbb{R}^n,\ \xi \in \mathbb{R}^m \end{aligned} \tag{10}$$

where A and C are matrices of proper dimension and A has full rank. There are two kinds of inputs: the first input u is Lipschitz continuous and can take any value in $\mathcal{U} \subset \mathbb{R}^n$ for which no probability distribution is known. The second input $\xi \in \mathbb{R}^m$ is white Gaussian noise. The combination of both inputs can be seen as a white Gaussian noise input, where the mean value is unknown within the set $\mathcal{U}$.

In contrast to the other system classes, we compute enclosing probabilistic hulls, i.e. a hull over all possible probability distributions when some parameters are uncertain and do not have a probability distribution. In the probabilistic setting ($C \neq 0$), the probability density function (PDF) at time $t = r$ of the random process $\mathbf{X}(t)$ defined by (10) for a specific trajectory $u(t) \in \mathcal{U}$ is denoted by $f_{\mathbf{X}}(x, r)$. The *enclosing probabilistic hull* (EPH) of all possible probability density functions $f_{\mathbf{X}}(x, r)$ is denoted by $\bar{f}_{\mathbf{X}}(x, r)$ and defined as: $\bar{f}_{\mathbf{X}}(x, r) = \sup\{f_{\mathbf{X}}(x, r) | \mathbf{X}(t)$ is a solution of (10) $\forall t \in [0, r]$, $u(t) \in \mathcal{U}$, $f_{\mathbf{X}}(x, 0) = f_0\}$. The enclosing probabilistic hull for a time interval is defined as $\bar{f}_{\mathbf{X}}(x, [0, r]) = \sup\{\bar{f}_{\mathbf{X}}(x, t) | t \in [0, r]\}$.

4.5 Nonlinear Systems

So far, reachable sets of linear continuous systems have been presented. Although a fairly large group of dynamic systems can be described by linear continuous systems, the extension to nonlinear continuous systems is an important step for the analysis of more complex systems. The analysis of nonlinear systems is much more complicated since many valuable properties are no longer valid. One of them is the superposition principle, which allows the homogeneous and the inhomogeneous solution to be obtained separately. Another is that reachable sets of linear systems can be computed by a linear map. This makes it possible to exploit that geometric representations such as ellipsoids, zonotopes, and polytopes are closed under linear transformations, i.e. they are again mapped to ellipsoids, zonotopes and polytopes, respectively. In CORA, reachability analysis of nonlinear systems is based on abstraction. We present abstraction by linear systems as presented in [1, Section 3.4] and by polynomial systems as presented in [2]. Since the abstraction causes additional errors, the abstraction errors are determined in an over-approximative way and added as an additional uncertain input so that an over-approximative computation is ensured.

General nonlinear continuous systems with uncertain parameters and Lipschitz continuity are considered. In analogy to the previous linear systems, the initial state $x(0)$ can take values from a set $\mathcal{X}_O \subset \mathbb{R}^n$ and the input u takes values from a set $\mathcal{U} \subset \mathbb{R}^m$. The evolution of the state x is defined by the following differential equation:

$$\dot{x}(t) = f(x(t), u(t)), \qquad x(0) \in \mathcal{X}_O \subset \mathbb{R}^n, \quad u(t) \in \mathcal{U} \subset \mathbb{R}^m,$$

where $u(t)$ and $f(x(t), u(t))$ are assumed to be globally Lipschitz continuous so that the Taylor expansion for the state and the input can always be computed, a condition required for the abstraction.

A brief visualization of the overall concept for computing the reachable set is shown in Fig. 8. As in the previous approaches, the reachable set is computed iteratively for time intervals $t \in \tau_k = [k\,r, (k+1)r]$ where $k \in \mathbb{N}^+$. The procedure for computing the reachable sets of the consecutive time intervals is as follows:

① The nonlinear system $\dot{x}(t) = f(x(t), u(t))$ is either abstracted to a linear system as shown

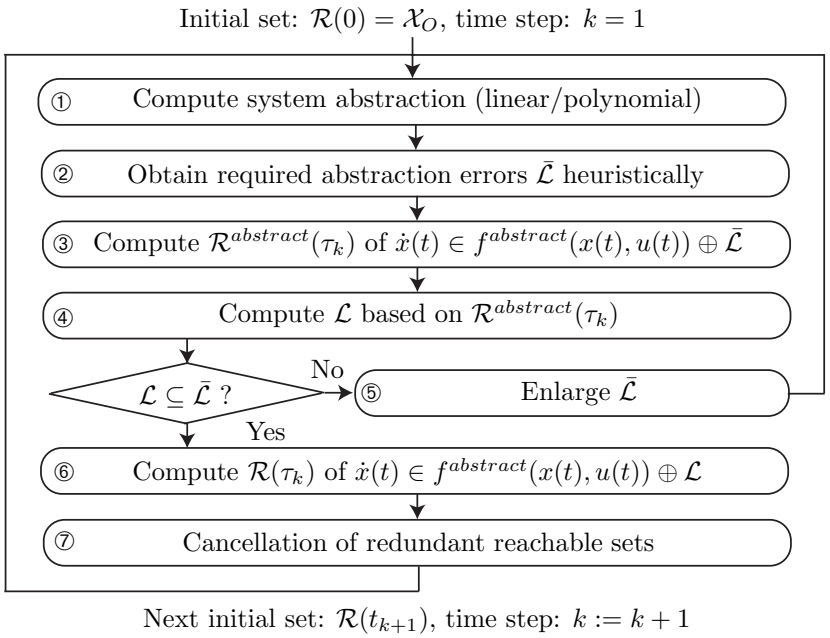


Figure 8: Computation of reachable sets – overview.

in (6) or after introducing $z = [x^T, u^T]^T$ a polynomial system of the form

$$\begin{aligned} \dot{x}_i = f^{abstract}(x, u) =& w_i + \frac{1}{1!}\sum_{j=1}^{o} C_{ij} z_j(t) + \frac{1}{2!}\sum_{j=1}^{o}\sum_{k=1}^{o} D_{ijk} z_j(t) z_k(t) \\ &+ \frac{1}{3!}\sum_{j=1}^{o}\sum_{k=1}^{o}\sum_{l=1}^{o} E_{ijkl} z_j(t) z_k(t) z_l(t) + \dots \end{aligned} \tag{11}$$

The set of abstraction errors $\mathcal{L}$ ensures that $f(x, u) \in f^{abstract}(x, u) \oplus \mathcal{L}$, which allows the reachable set to be computed in an over-approximative way.

② Next, the set of required abstraction errors $\bar{\mathcal{L}}$ is obtained heuristically.

③ The reachable set $\mathcal{R}^{abstract}(\tau_k)$ of $\dot{x}(t) \in f^{abstract}(x(t), u(t)) \oplus \bar{\mathcal{L}}$ is computed.

④ The set of abstraction errors $\mathcal{L}$ is computed based on the reachable set $\mathcal{R}^{abstract}(\tau_k)$.

⑤ When $\mathcal{L} \not\subseteq \bar{\mathcal{L}}$, the abstraction error is not admissible, requiring the assumption $\bar{\mathcal{L}}$ to be enlarged. If several enlargements are not successful, one has to split the reachable set and continue with one more partial reachable set from then on.

⑥ If $\mathcal{L} \subseteq \bar{\mathcal{L}}$, the abstraction error is accepted and the reachable set is obtained by using the tighter abstraction error: $\dot{x}(t) \in f^{abstract}(x(t), u(t)) \oplus \mathcal{L}$.

⑦ It remains to increase the time step ($k := k + 1$) and cancel redundant reachable sets that are already covered by previously computed reachable sets. This decreases the number of reachable sets that have to be considered in the next time interval.

The method `initReach` computes the reachable set for a first point in time r and the first time interval $[0, r]$. In contrast to linear systems, it is required to call `initReach` for each time

interval τ_k since the system is abstracted for each time interval τ_k by a different abstraction $f^{abstract}(x,u)$.

4.6 Nonlinear Systems with Uncertain Fixed Parameters

The class `nonlinParamSys` extends the class `nonlinearSys` by considering uncertain parameters p:

$$\dot{x}(t) = f(x(t), u(t), p), \qquad x(0) \in \mathcal{X}_O \subset \mathbb{R}^n, \quad u(t) \in \mathcal{U} \subset \mathbb{R}^m, \quad p \in \mathcal{P} \subset \mathbb{R}^p.$$

The functionality provided is identical to `nonlinearSys`, except that the abstraction to polynomial systems is not yet implemented.

4.7 Nonlinear Differential-Algebraic Systems

The class `nonlinDASys` considers time-invariant, semi-explicit, index-1 DAEs without parametric uncertainties since they are not yet implemented. The extension to parametric uncertainties can be done using the methods applied in Sec. 4.6. Using the vectors of differential variables x, algebraic variables y, and inputs u, the semi-explicit DAE can generally be written as

$$\begin{aligned} \dot{x} &= f(x(t), y(t), u(t)) \\ 0 &= g(x(t), y(t), u(t)), \\ [x^T(0), y^T(0)]^T &\in \mathcal{R}(0), \quad u(t) \in \mathcal{U}, \end{aligned} \tag{12}$$

where $\mathcal{R}(0)$ over-approximates the set of consistent initial states and $\mathcal{U}$ is the set of possible inputs. The initial state is consistent when $g(x(0), y(0), u(0)) = 0$, while for DAEs with an index greater than 1, further hidden algebraic constraints have to be considered [12, Chapter 9.1]. For an implicit DAE, the index-1 property holds if and only if $\forall t : \det(\frac{\partial g(x(t),y(t),u(t))}{\partial y}) \neq 0$, i.e. the Jacobian of the algebraic equations is non-singular [20, p. 34]. Loosely speaking, the index specifies the distance to an ODE (which has index 0) by the number of required time differentiations of the general form $0 = F(\dot{\tilde{x}}, \tilde{x}, u, t)$ along a solution $\tilde{x}(t)$, in order to express $\dot{\tilde{x}}$ as a continuous function of $\tilde{x}$ and t [12, Chapter 9.1].

To apply the methods presented in the previous section to compute reachable sets for DAEs, an abstraction of the original nonlinear DAEs to linear differential inclusions is performed for each consecutive time interval τ_k. A different abstraction is used for each time interval to minimize the over-approximation error. Based on a linearization of the functions $f(x(t), y(t), u(t))$ and $g(x(t), y(t), u(t))$, one can abstract the dynamics of the original nonlinear DAE by a linear system plus additive uncertainty as detailed in [7, Section IV]. This linear system only contains dynamic state variables x and uncertain inputs u. The algebraic state y is obtained afterwards by the linearized constraint function $g(x(t), y(t), u(t))$ as described in [7, Proposition 2].

5 Hybrid Dynamics

In CORA, hybrid systems are modeled by hybrid automata. Besides a continuous state x, there also exists a discrete state v for hybrid systems. The continuous initial state may take

values within continuous sets while only a single initial discrete state is assumed without loss of generality[23]. The switching of the continuous dynamics is triggered by *guard sets*. Jumps in the continuous state are considered after the discrete state has changed. One of the most intuitive examples where jumps in the continuous state can occur is the bouncing ball example (see Sec. 7), where the velocity of the ball changes instantaneously when hitting the ground.

The formal definition of the hybrid automaton is similarly defined as in [49]. The main difference is the consideration of uncertain parameters and the restrictions on jumps and guard sets. A hybrid automaton $HA = (\mathcal{V}, v^0, \mathcal{X}, \mathcal{X}^0, \mathcal{U}, \mathcal{P}, \texttt{inv}, \texttt{T}, \texttt{g}, \texttt{h}, \texttt{f})$, as it is considered in CORA, consists of:

- the finite set of locations $\mathcal{V} = \{v_1, \dots, v_\xi\}$ with an initial location $v^0 \in \mathcal{V}$.
- the continuous state space $\mathcal{X} \subseteq \mathbb{R}^n$ and the set of initial continuous states $\mathcal{X}^0$ such that $\mathcal{X}^0 \subseteq \texttt{inv}(v^0)$.
- the continuous input space $\mathcal{U} \subseteq \mathbb{R}^m$.
- the parameter space $\mathcal{P} \subseteq \mathbb{R}^p$.
- the mapping[24] $\texttt{inv}$: $\mathcal{V} \to 2^{\mathcal{X}}$, which assigns an invariant $\texttt{inv}(v) \subseteq \mathcal{X}$ to each location v.
- the set of discrete transitions $\texttt{T} \subseteq \mathcal{V} \times \mathcal{V}$. A transition from $v_i \in \mathcal{V}$ to $v_j \in \mathcal{V}$ is denoted by (v_i, v_j).
- the guard function $\texttt{g} : \texttt{T} \to 2^{\mathcal{X}}$, which associates a guard set $\texttt{g}((v_i, v_j))$ for each transition from v_i to v_j, where $\texttt{g}((v_i, v_j)) \cap \texttt{inv}(v_i) \neq \emptyset$.
- the jump function $\texttt{h} : \texttt{T} \times \mathcal{X} \to \mathcal{X}$, which returns the next continuous state when a transition is taken.
- the flow function $\texttt{f} : \mathcal{V} \times \mathcal{X} \times \mathcal{U} \times \mathcal{P} \to \mathbb{R}^{(n)}$, which defines a continuous vector field for the time derivative of x: $\dot{x} = \texttt{f}(v, x, u, p)$.

The invariants $\texttt{inv}(v)$ and the guard sets $\texttt{g}((v_i, v_j))$ are modeled by polytopes. The jump function is restricted to a linear map

$$x' = K_{(v_i,v_j)}\, x + l_{(v_i,v_j)}, \tag{13}$$

where x' denotes the state after the transition is taken and $K_{(v_i,v_j)} \in \mathbb{R}^{n \times n}$, $l_{(v_i,v_j)} \in \mathbb{R}^n$ are specific for a transition (v_i, v_j). The input sets $\mathcal{U}_v$ are modeled by zonotopes and are also dependent on the location v. Note that in order to use the results from reachability analysis of nonlinear systems, the input $u(t)$ is assumed to be locally Lipschitz continuous. The set of parameters $\mathcal{P}_v$ can also be chosen differently for each location v.

The evolution of the hybrid automaton is described informally as follows. Starting from an initial location $v(0) = v^0$ and an initial state $x(0) \in \mathcal{X}^0$, the continuous state evolves according to the flow function that is assigned to each location v. If the continuous state is within a guard set, the corresponding transition can be taken and has to be taken if the state would otherwise leave the invariant $\texttt{inv}(v)$. When the transition from the previous location v_i to the next location v_j is taken, the system state is updated according to the jump function and the continuous evolution within the next invariant.

Because the reachability of discrete states is simply a question of determining if the continuous reachable set hits certain guard sets, the focus of CORA is on the continuous reachable sets.

[23] In the case of several initial discrete states, the reachability analysis can be performed for each discrete state separately.

[24] $2^{\mathcal{X}}$ is the power set of $\mathcal{X}$.

Clearly, as for the continuous systems, the reachable set of the hybrid system has to be over-approximated in order to verify the safety of the system. An illustration of a reachable set of a hybrid automaton is given in Fig. 9.

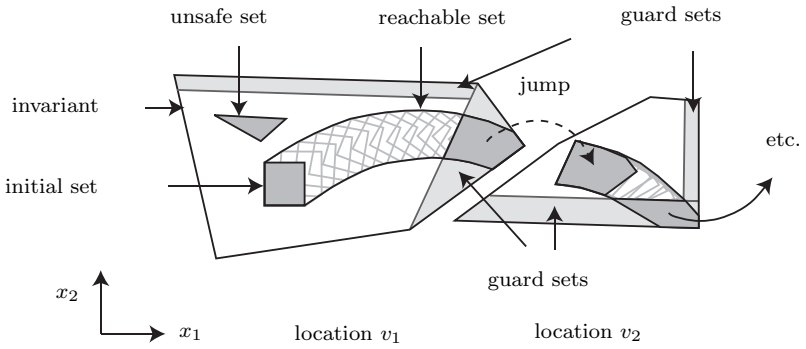


Figure 9: Illustration of the reachable set of a hybrid automaton.

5.1 Hybrid Automaton

A hybrid automaton is implemented as a collection of `locations`. We mainly support the following methods for hybrid automata:

- `hybridAutomaton` – constructor of the class.
- `plot` – plots the reachable set of the hybrid automaton.
- `reach` – computes the reachable set of the hybrid automaton.
- `simulate` – computes a hybrid trajectory of the hybrid automaton.

5.2 Location

Each location consists of:

- `invariant` – specified by a set representation of Sec. 2.
- `transitions` – cell array of objects of the class `transition`.
- `contDynamics` – specified by a continuous dynamics of Sec. 4.
- `name` – saved as a string describing the location.
- `id` – unique number of the location.

The supported methods of the `location` class are listed in Tab. 11.

5.3 Transition

Each transition consists of

- `guard` – specified by a set representation of Sec. 2.
- `reset` – struct containing the information for a linear reset.

Table 11: Most important methods of the class `location`.

name	description
`display`	displays the parameters of the location in the MATLAB workspace.
`enclosePolytopes`	encloses a set of polytopes using different over-approximating zonotopes.
`guardIntersect`	intersects the reachable sets with potential guard sets and returns enclosing zonotopes for each guard set.
`location`	constructor of the class.
`potInt`	determines which reachable sets potentially intersect with guard sets of a location.
`reach`	computes the reachable set for the location.
`simulate`	produces a single trajectory by solving the system numerically within the location starting from a point rather than from a set.

- `target` – `id` of the target location when the transition occurs.
- `inputLabel` – input event to communicate over events.
- `outputLabel` – output event to communicate over events.

We mainly support the following methods for transitions:

- `display` – displays the parameters of the transition in the MATLAB workspace.
- `reset` – computes the reset map after a transition occurs (also called 'jump function').

6 State Space Partitioning

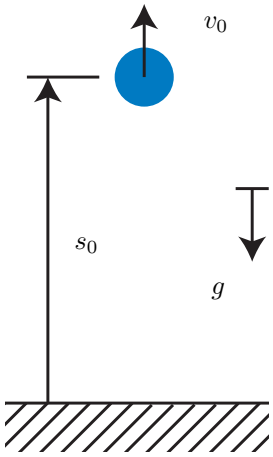
It is sometimes useful to partition the state space into cells, for instance, when abstracting a continuous stochastic system by a discrete stochastic system. CORA supports axis-aligned partitioning using the class `partition`. The main methods can be found in Tab. 12.

Table 12: Most important methods of the class `partition`.

name	description
`cellCandidates`	finds possible cells that might intersect with a continuous set over-approximated by its bounding box (interval hull).
`cellCenter`	returns center of specified cell.
`cellIndices`	returns cell indices given a set of cell coordinates.
`cellIntersection2`	returns the volumes of a polytope P intersected with touched cells C_i.
`cellSegment`	returns cell coordinates given a set of cell indices.
`display`	displays the parameters of the partition in the MATLAB workspace.
`findSegment`	finds segment index for given state space coordinates.
`findSegments`	return segment indices intersecting with a given interval hull.
`nrOfStates`	returns the number of discrete states of the partition.
`partition`	constructor of the class.
`segmentIntervals`	returns intervals of segment.
`segmentPolytope`	returns polytope of segment.
`segmentZonotope`	returns zonotope of segment.

7 Bouncing Ball Example

We demonstrate the syntax of CORA for the well-known bouncing ball example, see e.g. [51, Section 2.2.3]. Given is a ball in Fig. 10 with dynamics $\ddot{s} = -g$, where s is the vertical position and g is the gravity constant. After impact with the ground at $s = 0$, the velocity changes to $v' = -\alpha v$ ($v = \dot{s}$) with $\alpha \in [0, 1]$. The corresponding hybrid automaton can be formalized according to Sec. 5 as



$$
\begin{aligned}
\mathcal{V} &= \{v_1\} \\
\mathcal{X} &= \mathbb{R}^+ \times \mathbb{R} \quad \text{(ball is above ground)} \\
\mathcal{U} = \mathcal{Y}_c &= \{\} \\
\mathtt{T} &= \{(z_1, z_1)\} \\
\mathtt{inv}(z_1) &= \{[x_1, x_2]^T | x_1 \in \mathbb{R}_0^+, x_2 \in \mathbb{R}\} \\
\mathtt{g}\big((z_1, z_1)\big) &= \{[x_1, x_2]^T | x_1 = 0, x_2 \in \mathbb{R}_0^-\} \\
\mathtt{h}\big((z_1, z_1), x\big) &= \begin{bmatrix} x_1 \\ -\alpha\, x_2 \end{bmatrix} \\
\mathtt{f}(z_1, x) &= \begin{bmatrix} x_2 \\ -g \end{bmatrix}
\end{aligned}
$$

Figure 10: Bouncing ball.

The MATLAB code that implements the simulation and reachability analysis of the bouncing ball example is:

```
function bouncingBall()

%set options---------------------------------------------------------------
options.x0 = [1; 0]; %initial state for simulation
options.R0 = zonotope([options.x0, diag([0.05, 0.05])]); %initial set
options.startLoc = 1; %initial location
options.finalLoc = 0; %0: no final location
options.tStart = 0; %start time
options.tFinal = 5; %final time
options.timeStepLoc{1} = 0.05; %time step size in location 1
options.taylorTerms = 10;
options.zonotopeOrder = 20;
options.polytopeOrder = 10;
options.errorOrder=2;
options.reductionTechnique = 'girard';
options.isHybrid = 1;
options.isHyperplaneMap = 0;
options.enclosureEnables = [5]; %choose enclosure method(s)
options.originContained = 0;
options.polytopeType = 'mpt';
%--------------------------------------------------------------------------

```

```
%specify hybrid automaton-----------------------------------------------------
%define large and small distance
dist = 1e3;
eps = 1e-6;

A = [0 1; 0 0]; % system matrix
B = eye(2); % input matrix
linSys = linearSys('linearSys',A,B); %linear continuous system

inv = intervalhull([-2*eps, dist; -dist, dist]); %invariant
guard = intervalhull([- eps, 0; -dist, 0]); %guard set
reset.A = [0, 0; 0, -0.75]; reset.b = zeros(2,1); %reset
trans{1} = transition(guard,reset,1,'a','b'); %transition
loc{1} = location('loc1',1,inv,trans,linSys); %location
HA = hybridAutomaton(loc); % select location for hybrid automaton
%------------------------------------------------------------------------------

%set input:
options.uLoc{1} = [0; -1]; %input for simulation
options.uLocTrans{1} = options.uLoc{1}; %center of input set
options.Uloc{1} = zonotope(zeros(2,1)); %input deviation from center

%simulate hybrid automaton
HA = simulate(HA,options);

%compute reachable set
[HA] = reach(HA,options);

%choose projection and plot----------------------------------------------------
options.projectedDimensions = [1 2];
options.plotType = 'b';
plot(HA,'reachableSet',options); %plot reachable set
plot(options.R0,options.projectedDimensions,'blackFrame'); %plot initial set
plot(HA,'simulation',options); %plot simulation
%------------------------------------------------------------------------------
```

The reachable set and the simulation are plotted in Fig. 11 for a time horizon of $t_f = 5$ seconds.

8 Conclusions

CORA is a toolbox for the implementation of prototype reachability analysis algorithms in MATLAB. The software is modular and is organized into four main categories: vector set representations, matrix set representations, continuous dynamics, and hybrid dynamics. CORA includes novel algorithms for reachability analysis of nonlinear systems and hybrid systems with a special focus on scalability; for instance, a power network with more than 50 continuous state variables has been verified in [3]. The efficiency of the algorithms used means it is even possible to verify problems online, i.e. while they are in operation [5].

One particularly useful feature of CORA is its adaptability: the algorithms can be tailored to the reachability analysis problem in question. Forthcoming integration into SpaceEx, which has

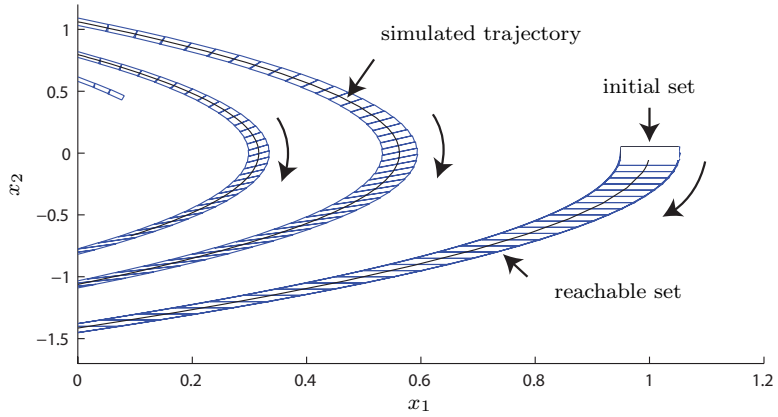


Figure 11: Illustration of the reachable set of the bouncing ball. The black box shows the initial set and the black line shows the simulated trajectory.

a user interface and a model editor, should go some way towards making CORA more accessible to non-experts.

Acknowledgment

The author gratefully acknowledges financial support by the European Commission project UnCoVerCPS under grant number 643921.

References

[1] M. Althoff. *Reachability Analysis and its Application to the Safety Assessment of Autonomous Cars*. Dissertation, Technische Universität München, 2010. http://nbn-resolving.de/urn/resolver.pl?urn:nbn:de:bvb:91-diss-20100715-963752-1-4.

[2] M. Althoff. Reachability analysis of nonlinear systems using conservative polynomialization and non-convex sets. In *Hybrid Systems: Computation and Control*, pages 173–182, 2013.

[3] M. Althoff. Formal and compositional analysis of power systems using reachable sets. *IEEE Transactions on Power Systems*, 29(5):2270–2280, 2014.

[4] M. Althoff and J. M. Dolan. Reachability computation of low-order models for the safety verification of high-order road vehicle models. In *Proc. of the American Control Conference*, pages 3559–3566, 2012.

[5] M. Althoff and J. M. Dolan. Online verification of automated road vehicles using reachability analysis. *IEEE Transactions on Robotics*, 30(4):903–918, 2014.

[6] M. Althoff and B. H. Krogh. Zonotope bundles for the efficient computation of reachable sets. In *Proc. of the 50th IEEE Conference on Decision and Control*, pages 6814–6821, 2011.

[7] M. Althoff and B. H. Krogh. Reachability analysis of nonlinear differential-algebraic systems. *IEEE Transactions on Automatic Control*, 59(2):371–383, 2014.

[8] M. Althoff, B. H. Krogh, and O. Stursberg. *Modeling, Design, and Simulation of Systems with Uncertainties*, chapter Analyzing Reachability of Linear Dynamic Systems with Parametric Uncertainties, pages 69–94. Springer, 2011.

[9] M. Althoff, C. Le Guernic, and B. H. Krogh. Reachable set computation for uncertain time-varying linear systems. In *Hybrid Systems: Computation and Control*, pages 93–102, 2011.

[10] M. Althoff, O. Stursberg, and M. Buss. Safety assessment for stochastic linear systems using enclosing hulls of probability density functions. In *Proc. of the European Control Conference*, pages 625–630, 2009.

[11] E. Asarin, T. Dang, and O. Maler. d/dt: A verification tool for hybrid systems. In *Proc. of the Conference on Decision and Control*, pages 2893–2898, 2001.

[12] U. M. Ascher and L. R. Petzold. *Computer Methods for Ordinary Differential Equations and Differential-Algebraic Equations*. SIAM: Society for Industrial and Applied Mathematics, 1998.

[13] G. Behrmann, A. David, K. G. Larsen, O. Möller, P. Pettersson, and W. Yi. UPPAAL - present and future. In *Proc. of the 40th IEEE Conference on Decision and Control*, pages 2881 – 2886, 2001.

[14] L. Benvenuti, D. Bresolin, P. Collins, A. Ferrari, L. Geretti, and T. Villa. *Reachability Problems*, chapter Ariadne: Dominance Checking of Nonlinear Hybrid Automata Using Reachability Analysis, pages 79–91. Springer, 2012.

[15] L. Benvenuti, D. Bresolin, P. Collins, A. Ferrari, L. Geretti, and T. Villa. Assume-guarantee verification of nonlinear hybrid systems with ARIADNE. *International Journal of Robust and Nonlinear Control*, 24:699–724, 2014.

[16] D. Berleant. Automatically verified reasoning with both intervals and probability density functions. *Interval Computations*, 2:48–70, 1993.

[17] M. Berz and G. Hoffstätter. Computation and application of Taylor polynomials with interval remainder bounds. *Reliable Computing*, 4:83–97, 1998.

[18] N. S. Bjørner, A. Browne, M. A. Colón, B. Finkbeiner, Z. Manna, H. B. Sipma, and T. E. Uribe. Verifying temporal properties of reactive systems: A STeP tutorial. *Formal Methods in System Design*, 16(3):227–270, 2000.

[19] O. Botchkarev and S. Tripakis. Verification of hybrid systems with linear differential inclusions using ellipsoidal approximations. In *Hybrid Systems: Computation and Control*, LNCS 1790, pages 73–88. Springer, 2000.

[20] K. E. Brenan, S. L. Campbell, and L. R. Petzold. *Numerical Solution of Initial Value Problems in Differential-Algebraic Equations*. North-Holland, 1989.

[21] X. Chen, E. Abraham, and S. Sankaranarayanan. Flow*: An analyzer for non-linear hybrid systems. In *Proc. of Computer-Aided Verification*, LNCS 8044, pages 258–263. Springer, 2013.

[22] X. Chen, S. Sankaranarayanan, and E. Ábrahám. Taylor model flowpipe construction for non-linear hybrid systems. In *Proc. of the 33rd IEEE Real-Time Systems Symposium*, 2012.

[23] A. Chutinan and B. H. Krogh. Computational techniques for hybrid system verification. *IEEE Transactions on Automatic Control*, 48(1):64–75, 2003.

[24] M. Fränzle and C. Herde. HySAT: An efficient proof engine for bounded model checking of hybrid systems. *Formal Methods in System Design*, 30(3):179–198, 2007.

[25] G. Frehse. PHAVer: Algorithmic verification of hybrid systems past HyTech. *International Journal on Software Tools for Technology Transfer*, 10:263–279, 2008.

[26] G. Frehse, C. Le Guernic, A. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, and O. Maler. SpaceEx: Scalable verification of hybrid systems. In *Proc. of the 23rd International Conference on Computer Aided Verification*, LNCS 6806, pages 379–395. Springer, 2011.

[27] G. Frehse and R. Ray. Flowpipe-guard intersection for reachability computations with support functions. In *Proc. of Analysis and Design of Hybrid Systems*, pages 94–101, 2012.

[28] S. Gao, S. Kong, and E. Clarke. dReal: An SMT solver for nonlinear theories of the reals. In

Proc. of the Conference on Automated Deduction, 2013.

[29] S. Gao, S. Kong, and E. Clarke. Satisfiability modulo ODEs. In *Proc. of Formal Methods in Computer-Aided Design*, pages 105–112, 2013.

[30] C. W. Gardiner. *Handbook of Stochastic Methods: For Physics, Chemistry and the Natural Sciences*. Springer, 1983.

[31] A. Girard. Reachability of uncertain linear systems using zonotopes. In *Hybrid Systems: Computation and Control*, LNCS 3414, pages 291–305. Springer, 2005.

[32] A. Girard and C. Le Guernic. Efficient reachability analysis for linear systems using support functions. In *Proc. of the 17th IFAC World Congress*, pages 8966–8971, 2008.

[33] A. Girard, C. Le Guernic, and O. Maler. Efficient computation of reachable sets of linear time-invariant systems with inputs. In *Hybrid Systems: Computation and Control*, LNCS 3927, pages 257–271. Springer, 2006.

[34] E. Gover and N. Krikorian. Determinants and the volumes of parallelotopes and zonotopes. *Linear Algebra and its Applications*, 433(1):28–40, 2010.

[35] T. A. Henzinger, P.-H. Ho, and H. Wong-Toi. HyTech: A model checker for hybrid systems. *Software Tools for Technology Transfer*, 1:110–122, 1997.

[36] T. A. Henzinger, B. Horowitz, R. Majumdar, and H. Wong-Toi. Beyond HyTech: Hybrid systems analysis using interval numerical methods. In *Hybrid Systems: Computation and Control*, LNCS 1790, pages 130–144. Springer, 2000.

[37] J. Hoefkens, M. Berz, and K. Makino. *Automatic Differentiation: From Simulation to Optimization*, chapter Efficient High-Order Methods for ODEs and DAEs, pages 343–348. Springer, 2001.

[38] J. Hoefkens, M. Berz, and K. Makino. *Scientific Computing, Validated Numerics, Interval Methods*, chapter Verified High-Order Integration of DAEs and Higher-Order ODEs, pages 281–292. Springer, 2001.

[39] V. Kaibel and M. E. Pfetsch. *Algebra, Geometry and Software Systems*, chapter Some Algorithmic Problems in Polytope Theory, pages 23–47. Springer, 2003.

[40] S. Kowalewski and H. Treseler. VERDICT - a tool for model-based verification of real-time logic process controllers. In *Proc. of the Joint Workshop on Parallel and Distributed Real-Time Systems*, pages 217–221, 1997.

[41] A. A. Kurzhanskiy and P. Varaiya. *The Control Handbook*, chapter Computation of Reach Sets for Dynamical Systems. CRC Press, 2010.

[42] G. Lafferriere, G. J. Pappas, and S. Yovine. Symbolic reachability computation for families of linear vector fields. *Symbolic Computation*, 32:231–253, 2001.

[43] I. M. Mitchell. The flexible, extensible and efficient toolbox of level set methods. *Journal of Scientific Computing*, 35(2-3):300–329, 2008.

[44] I. M. Mitchell, A. M. Bayen, and C. J. Tomlin. A time-dependent Hamilton–Jacobi formulation of reachable sets for continuous dynamic games. *IEEE Transactions on Automatic Control*, 50:947–957, 2005.

[45] N. S. Nedialkov. *Modeling, Design, and Simulation of Systems with Uncertainties.*, volume 3, chapter Implementing a Rigorous ODE Solver through Literate Programming, pages 3–19. Springer, 2011.

[46] A. Platzer. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*. Springer, 2010.

[47] A. Platzer and J.-D. Quesel. KeYmaera: A hybrid theorem prover for hybrid systems. In *Proc. of the Fourth International Joint Conference on Automated Reasoning*, volume 5195 of *LNCS*, pages 171–178. Springer, 2008.

[48] S. Ratschan and Z. She. Safety verification of hybrid systems by constraint propagation based abstraction refinement. *ACM Transactions in Embedded Computing Systems*, 6(1):1–23, 2007.

[49] O. Stursberg and B. H. Krogh. Efficient representation and computation of reachable sets for hybrid

systems. In *Hybrid Systems: Computation and Control*, LNCS 2623, pages 482–497. Springer, 2003.

[50] S. Tripakis, S. Yovine, and A. Bouajjani. Checking timed Büchi automata emptiness efficiently. *Formal Methods in System Design*, 26(3):267–292, 2005.

[51] A. van der Schaft and H. Schumacher. *An Introduction to Hybrid Dynamical Systems*. Springer, 2000.

[52] G. M. Ziegler. *Lectures on Polytopes*. Graduate Texts in Mathematics. Springer, 1995.