Verification of Uncertain Embedded Systems by Computing Reachable Sets based on Zonotopes

Matthias Althoff * **Olaf Stursberg** * **Martin Buss** *

* *Institute of Automatic Control Engineering (LSR) , Technische Universität München, 80290 München, Germany.*
Email: {althoff,stursberg,mb}@ tum.de.

Abstract: Formal verification using reachability analysis has been shown to be useful for detecting design failures for controlled embedded systems, and thus to improve dependability. If the state space is hybrid, however, the growth of complexity with the dimension of the continuous dynamics limits the applicability significantly. This paper proposes an efficient approach to computing reachable sets for hybrid systems with time-varying linear continuous dynamics and uncertain inputs. The key idea is to combine zonotopes and polytopes for set representation when reachable sets are intersected with the transition guards which determine the discrete behavior of the hybrid system. Different methods for conservatively transforming zonotopes into polytopes (and vice versa) are proposed and experimentally compared.

Keywords: Dependability, hybrid systems, reachability analysis, verification.

1. INTRODUCTION

When formal verification is used to determine design failures of controlled embedded systems, it can contribute to enhancing the systems' dependability and reliability, as reported for discrete event models in several publications. If continuous dynamics must be considered for analysis in addition (i.e. if the behavior of the embedded system is hybrid), the verification is much more intricate. This is not only due to the infinity of the search space in this case, but small model-plant mismatches may lead to completely different hybrid behaviors and thus make the verification result obtained for the model meaningless. It is thus important to consider model uncertainty in analyzing whether an embedded system is dependable in the sense that its design meets given specifications. As opposed to testing techniques like Monte-Carlo simulation, which in the general case cannot prove model properties for all possible behaviors, this paper proposes an approach to algorithmically verifying safety for hybrid dynamics with uncertain model components. The method is based on a conservative computation of sets of reachable states – if this set does not intersect with a specified set of unsafe states, the model is proven to be safe. For computing reachable sets of hybrid systems without uncertain model parameters, several approaches have been published and they use different types of set representations: ellipsoids (Botchkarev and Tripakis [2000]), polytopes (Chutinan and Krogh [2003]), oriented rectangular hulls (Stursberg and Krogh [2003]) and zonotopes (Girard [2005]). Zonotopes are a special case of polytopes and were shown to be an efficient choice for representing and computing reachable sets in continuous spaces, see Girard [2005]. Zonotopes are the only known representation of reachable sets that allow to compute reachable sets of linear systems with up to at least 100 states in relatively short time (i.e. in a few minutes). The applicability of zonotopes has been extended in Althoff et al. [2007] to linear systems with uncertain system matrices as well as uncertain input and disturbance sets modeled as zonotopes.

In this paper, the method is further extended to account also for the discrete dynamics of hybrid systems: to compute reachable sets for hybrid dynamics, the intersection with guard sets (as the enabling continuous state sets for discrete transitions) has to be taken into account. Guard sets are typically modeled as general polytopes in many types of hybrid systems and for most applications. Even if guard sets cannot be modeled explicitly as polytopes, they can be over-approximated by polytopes and still allow to conclude on safety when used in verification. If the continuous reachable sets are represented by zonotopes and guard sets by polytopes, one has to consider that the intersection itself is not a zonotope in general; the same is true for the intersection of two zonotopes. This paper presents a solution to this problem by transforming the representation of a zonotope first into the one of polytopes. The intersection can then be carried out for polytopes, and the result is again over-approximated by a zonotope, such that the computation of the continuous reachable set can be continued using zonotopes.

The paper first introduces the investigated class of hybrid system (Sec. 2) and the definitions of polytopes and zonotopes (Sec. 3). After recalling the basic scheme for computing continuous reachable sets (Sec. 4), different alternatives for computing intersections and conservative transformation between zonotopes and polytopes are described as main contribution (Sec. 5). The paper closes with an application that illustrates the use in checking dependability for embedded systems.

2. PROBLEM STATEMENT

The presented methods for the computation of reachable sets are designed for hybrid automata $HA = (Z, z_0, X, X_0, inv, T, g, j, flow)$ with a syntax and semantics as defined in Stursberg and Krogh [2003]. This class of hybrid automata consists of a finite set of locations $Z \in \mathbb{N}^+$, an initial location $z_0 \in Z$, the continuous state space $X \subseteq \mathbb{R}^n$, an initial continuous set $X_0 \subseteq X$, and a set of discrete transitions $T \subseteq Z \times Z$. In this work, the invariant sets inv and the guard sets g are modeled as polytopes. The jump function j updates the continuous state according to $x' = C_g \cdot x + d_g$ when a transition is taken, where $C_g \in \mathbb{R}^{n \times n}$, $d_g \in \mathbb{R}^n$, and g is the index for the guard of the corresponding transition. To specify the continuous dynamics, the flow function $flow$ has here the form of a linear time-varying dynamics with uncertain inputs. The system matrix is modeled as an interval matrix $A(t) \in \mathcal{I}^{n \times n}$ with $\mathcal{I}$ as the set of all intervals $[c, d]$ and $c, d \in \mathbb{R}$, $c \leq d$. For the system matrix applies $A(t) \in \langle \underline{A}, \overline{A} \rangle$ when $\underline{A}, \overline{A} \in \mathbb{R}^{n \times n}$ are the matrices determining the left and right limits of the intervals in A, i.e. for each element of A: $\underline{a}_{ij} \leq \overline{a}_{ij}, \forall i, j = 1, \ldots, n$ (with i and j denoting the row and column of A). The coefficients of $A(t)$ can vary independently over time $t \in \mathbb{R}^+$ and the time-varying input $v(t)$ is restricted to a set V:

$$\dot{x} = A(t)x + v(t), \quad x(0) \in X_0 \subset \mathbb{R}^n, v(t) \in V \subset \mathbb{R}^n. \quad (1)$$

The over-approximated set of states reachable for (1) in a time interval $t \in [0, r]$ is defined over the reachable set at a time point $t = r$ and for all possible Lipschitz continuous input trajectories with $v(t) \in V$, $t \in [0, r]$:

Definition 1. $R(r)$ is an over-approximation of the exact reachable set $R^e(r)$ that can be reached starting from X_0 (for $t = 0$) at time $t = r$:

$$R^e(r) = \{x | x(t) \text{ is solution of } (1),\ t = r\},\ R(r) \supseteq R^e(r).$$

Definition 2. $R([0, r])$ is the union of reachable sets $R(t)$ for $t \in [0, r]$: $R([0, r]) = \bigcup_{t \in [0,r]} R(t)$.

The considered problem is to compute the reachable continuous set of HA for given z_0, X_0, and for a time span $[0, t_f]$. Discrete transitions according to T occurring during this time span have to be considered by iterating through the following steps: (i) determining a continuous reachable set $R([0, r])$ according to Def. 2 for the current location z, (ii) computing the intersection of $R([0, r])$ and the guard sets of each transition leaving out of z, and (iii) applying the reset function of the corresponding transition to the intersection obtained in (ii). After executing step (i), the emptiness of the intersection of the continuous reachable set with a given set of unsafe states $X_u \subset X$ is checked – if this check fails, the system is identified to be unsafe.

3. PRELIMINARIES

This section reviews the definitions of polytopes and zonotopes. To define a polytope, the definition of a halfspace is introduced as: $S := \{x | c \cdot x \leq d, c \in \mathbb{R}^{1 \times n}, d \in \mathbb{R}\}$. For a given S, let $b := \{x | c \cdot x = d\}$ denote the corresponding bounding hyperplane. A polytope P is the nonempty intersection of a finite set $S := \{S_1, \ldots, S_q\}$ of halfspaces:

Definition 3. (Convex Polytope). For q halfspaces, a convex polytope P is the set:

$$P = \left\{ x \in \mathbb{R}^n : C \cdot x \leq d, \quad C \in \mathbb{R}^{q \times n}, d \in \mathbb{R}^{q \times 1} \right\}.$$

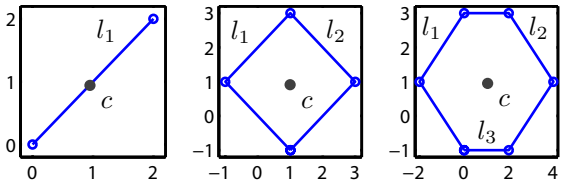
This representation of a polytope is also referred to as the *halfspace representation*. As zonotopes are a special case of polytopes, they can also be represented by halfspaces. A definition of zonotopes using so-called *generators* $g^{(1)}, \ldots, g^{(p)}$ is the following (see e.g. Ziegler [1995]):

Definition 4. (Zonotope). A zonotope is a set:

$$Z = \left\{ x \in \mathbb{R}^n : x = c + \sum_{i=1}^{p} x^{(i)} \cdot g^{(i)}, \quad -1 \leq x^{(i)} \leq 1 \right\}$$

with $c, g^{(1)}, \ldots, g^{(p)} \in \mathbb{R}^n$. The zonotope order is $q = \frac{p}{n}$.

This representation is referred to as the *generator representation*. An alternative definition of a zonotope is the Minkowski sum[1] of a finite set of line segments $l_i = [-1, 1] g^{(i)}$ (Girard [2005]). Fig. 1 shows how a zonotope is constructed for a two-dimensional case with three generators. Zonotopes are always centrally symmetric with center c.



(a) $c + l_1$ (b) $c + l_1 + l_2$ (c) $c + l_1 + l_2 + l_3$

Fig. 1. Construction of a zonotope.

4. OVER-APPROXIMATION OF REACHABLE SETS

The over-approximation of reachable sets is first discussed for purely continuous dynamics, and in the second part of this section, the intersection with guards is addressed. Most algorithms (e.g. Girard [2005], Chutinan and Krogh [2003], Stursberg and Krogh [2003], Althoff et al. [2007]) for continuous reachability analysis use the similar basic steps to compute the reachable set for time intervals $t \in [k \cdot r, (k + 1) \cdot r]$ for $k \in \{0, 1, \ldots, k_f\}$ and $r \in \mathbb{R}^+$:

(1) computation of the reachable sets at the time points $t = k \cdot r$ and $t = (k + 1) \cdot r$,
(2) generation of a convex hull of the two reachable sets,
(3) enlargement of the convex hull to ensure enclosure of all trajectories for the time interval $t \in [k \cdot r, (k+1) \cdot r]$.

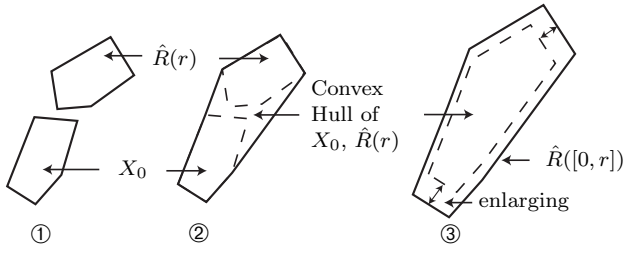


Fig. 2. Overview of computing of reachable sets.

[1] Minkowski sum of two sets A, B: $A \oplus B = \{a + b | a \in A, b \in B\}$

These basic steps are illustrated in Fig. 2. In this work, the reachable sets $R([k \cdot r, (k+1) \cdot r])$ are computed as proposed in Althoff et al. [2007]: Due to the linearity of the system (1), it is possible to separate the computation for the state and input dependent term of (1). The reachable set for the state dependent part, denoted by $\hat{R}([0, r])$, is computed by the steps 1 to 3 only for the first time interval $[0, r]$. The solution for intervals with $k > 1$, the set is computed by the multiplication of $\hat{R}([0, r])$ with the matrix exponential $e^{\mathcal{A} \cdot r}$ of the interval system matrix $\mathcal{A}$. As $e^{\mathcal{A} \cdot r}$ cannot be computed exactly for an interval matrix $\mathcal{A}$, an over-approximation $\lceil e_p^{\mathcal{A}t} \rceil$ is used, which is computed as presented in Althoff et al. [2007]. The index p refers to the number of Taylor terms used for the over-approximation. The reachable sets for $t \in [k \cdot r, (k+1) \cdot r]$ are:

$$\hat{R}([k \cdot r, (k+1) \cdot r]) = \lceil e_p^{\mathcal{A} \cdot k \cdot r} \rceil \cdot \hat{R}([0, r]).$$

Due to the superposition principle of linear systems, the reachable set of the input dependent part $\bar{R}([0, r])$ can be added to $\hat{R}([0, r])$ to obtain the overall solution:

$$R([0, r]) = \hat{R}([0, r]) + \bar{R}([0, r]).$$

With respect to the computation of $\bar{R}([0, r])$, the reader is referred to the procedure in Althoff et al. [2007]. The reachable set for $[0, k_f \cdot r]$ is the union of the reachable sets for the single time intervals:

$$R([0, T]) = \bigcup_{k=1}^{k_f} R([(k-1) \cdot r, k \cdot r]).$$

The procedure for computing the reachable set within one location of HA has to account for the intersection with the invariant set and guard sets. The algorithm for the computation in one location is shown in Algo. 1. The intersection of the reachable set with the i^{th} guard set is denoted R'_i . The set R'_i is then projected by the jump function j resulting in a set from which the continuous evolution in the next location is resumed. As the jump function is linear, the zonotopes are mapped to zonotopes as shown in Girard [2005]. The operator ⋒ in algorithm 1 denotes the over-approximation of an intersection. The over-approximation is necessary since the intersection of a reachable set segment (represented as a zonotope) with a polytope (invariant or guard) is a zonotope only in special cases. Thus, the resulting polytope has to be over-approximated by a zonotope to continue the computation of reachable sets with zonotopes. The procedure for intersecting a zonotope with a polytope and the over-approximation of the result by a zonotope is described next.

Algorithm 1 Compute R_z within a location $z \in Z$

Input: reachable set $R([0, r])$, invariant inv, o guard sets g_i
Output: R, R'_i
  $k := 2$
  while $R([(k-2) \cdot r, (k-1) \cdot r]) \neq \varnothing$ **do**
    $\hat{R}([(k-1)r, kr]) = \lceil e_p^{Ar} \rceil R([(k-2)r, (k-1)r])$
    $R([(k-1)r, kr]) = [\hat{R}([(k-1)r, kr]) + \bar{R}([0, r])] \text{⋒} inv$
    $k := k + 1$
  end while
  $t_m = (k-1)r$
  $R([0, t_m]) = \bigcup_{k=1}^{t_m/r} R([(k-1)r, kr])$
  for $i = 1 \ldots o$ **do**
    $R'_i = R([0, t_m]) \text{⋒} g_i$
  end for

5. INTERSECTION OF ZONOTOPES WITH POLYTOPES

Computing the intersection of two polytopes is possible by several algorithms. However, the computational complexity of transforming a zonotope to a halfspace representation of a polytope is high, i.e. obtaining a halfspace representation from a zonotope for a dimension 10 is already difficult in practice Fukuda [2004]. For this reason, methods to over-approximate zonotopes by parallelotopes (i.e. zonotope of order 1) are presented here. Parallelotopes can be directly transformed to a halfspace representation for dimensions greater than 10.

5.1 Conversion from Generators to Halfspace Representations of Parallelotopes

In order to formulate a method that directly transforms the generator representation of a parallelotope to a halfspace representation, the n-dimensional cross product is introduced. The n-dimensional cross product of $n-1$ vectors $h_i \in \mathbb{R}^n$ is defined as in Mortari [1996]: consider a matrix $H = [h_1, \ldots, h_{n-1}] \in \mathbb{R}^{n \times n-1}$, and let $H^{[i]} \in \mathbb{R}^{n-1 \times n-1}$ be the H-matrix in which the i^{th} row is removed.

Definition 5. (n-dimensional Cross Product).
The cross product operator $nX()$ is defined as follows:

$$y = nX(H) = \begin{bmatrix} \ldots & (-1)^{i+1} \det(H^{[i]}) & \ldots \end{bmatrix}^T$$

Analogously to the common three dimensional cross product, the n-dimensional cross product returns a vector that is orthogonal to the other $n-1$ vectors. It allows to formulate an instruction for the halfspace generation of a parallelotope:

Proposition 1. (Halfspace Representation of Parallelotopes). The halfspace representation $Cx \leq d$ of a parallelotope with n independent generators is

$$C = \begin{bmatrix} C^+ & -C^+ \end{bmatrix}^T, \quad d = \begin{bmatrix} d^+ & d^- \end{bmatrix}^T$$

with:

$$C_i^+ = nX(G^{\langle i \rangle})^T / \|nX(G^{\langle i \rangle})\|_2$$
$$d_i^+ = C_i^{+T}(c + \text{sign}(C_i^{+T} g^{(i)}) g^{(i)})$$
$$d_i^- = -C_i^{+T}(c - \text{sign}(C_i^{+T} g^{(i)}) g^{(i)})$$

and $G = \begin{bmatrix} g^{(1)} & \ldots g^{(n)} \end{bmatrix}$ is the matrix of the generators and $G^{\langle i \rangle}$ is defined as a matrix G in which the i^{th} column is removed. C_i^+ denotes the ith row of C^+.

Proof: A parallelotope can be represented by $2n$ halfspaces, where n is the dimension of the state space. The bounding hyperplanes b_i of the ith halfspace can be reached from the center c by translation of a single generator $g^{(i)}$: $c + g^{(i)} \in b_i$. As there are only n generators, the bounding hyperplane b_i must be spanned by the matrix of remaining generators $G^{\langle i \rangle}$. Thus, the normal vector C_i of b_i is computed as $C_i^+ = nX(G^{\langle i \rangle})^T / \|nX(G^{\langle i \rangle})\|_2$. It is sufficient to compute n halfspaces denoted by a superscript '+', as the

remaining n halfspaces denoted by a superscript '$-$' differ only in sign due to the central symmetry of zonotopes. The elements d_i^+ are the minimum distance from the origin to the bounding hyperplane b_i^+. As the vector to b_i^+ is known ($c+\text{sign}({C_i^+}^T g^{(i)})g^{(i)} \in b_i^+$), the minimum distance is computed by the projection of this vector onto the normalized normal vector C_i^+ by ${C_i^+}^T(c+\text{sign}({C_i^+}^T g^{(i)})g^{(i)})$, and analogously for the opposite halfspace. □

An alternative way to get a polytope representation of a first order zonotope is to compute the extreme points e_k by $e_k = c \pm g_1 .. \pm g_p$, $k \in \{1, \ldots, 2^n\}$ such that the resulting polytope is the convex hull of the extreme points. While the number of extreme points for a first order zonotope is 2^n, the number of halfspaces in proposition 1 is $2n$ only, i.e. the latter is preferable.

In order to compute over-approximations of zonotopes represented by polytopes, the computation of the interval hull of a zonotope is introduced. An interval hull $\mathcal{H} \in \mathcal{I}^n$ is a set that is spanned by the set of possible intervals $\mathcal{I}$ (see Sec. 2). An example of a three dimensional interval hull is a cube.

Proposition 2. (Interval Hull of a Zonotope). An interval hull $\mathcal{H}$ in generator representation is computed from a zonotope $Z = (c, g^{(1)}, \ldots, g^{(p)})$ by:

$$\mathcal{H} = \mathcal{IH}(Z) = (c, v^{(1)}, \ldots, v^{(n)})$$

with $v_j^{(i)} = 0$ for $i \neq j$ and $v_j^{(i)} = \sum_{k=1}^{p} |g_j|^{(k)}$ for $i = j$. The subscript j of $v_j^{(i)}$ denotes the j^{th} element of $v^{(i)}$.

Proof: The interval of possible values of an element of a single generator is $\left[-|g_j^{(i)}|, |g_j^{(i)}|\right]$. Summation of the intervals of each generator results into $\left[-\sum_{k=1}^{p} |g_j^{(k)}|, \sum_{k=1}^{p} |g_j^{(k)}|\right]$ for the j^{th} dimension. The interval of dimension j is represented by a generator $v^{(i)}$, where only the j^{th} element is nonzero. □

The over-approximation of zonotopes by interval hulls is computationally cheap and allows to efficiently over-approximate a zonotope of arbitrary order $q > 1$ to a parallelotope:

Proposition 3. (Order Reduction to a First Order Zonotope). An over-approximating parallelotope Ψ is obtained from a zonotope Z by:

$$\Psi = \Gamma \cdot \mathcal{IH}(\Gamma^{-1} Z)$$

where $\Gamma \in \mathbb{R}^{n \times n}$ is a matrix of n generators $g^{(i)}$ taken out of the set of all p generators.

This approach first transforms the coordinates of Z by the linear map Γ^{-1}, where the new coordinates are the n chosen generators within Γ. Note that this coordinate system is not orthogonal in general. Within this coordinate system, the zonotope is over-approximated by an interval hull ($\mathcal{IH}(\Gamma^{-1}Z)$). As a final step, the zonotope is transformed back to the original coordinate system. Due to the fact that the zonotope is over-approximated in the transformed coordinate system, it is over-approximated in the original coordinate system, too. Another view of this procedure is the following: A zonotope is constructed first of n out of p generators. Next, the chosen generators are enlarged by an amount ensuring the enclosure of the original zonotope. It remains to find a heuristics that select the generators of the matrix Γ of proposition 3 in a good (or the best) way.

5.2 Reduction Methods

This part proposes several methods to over-approximate a zonotope using parallelotopes. The methods differ in two ways: First, they use different criteria to pick the n generators determining the transformation matrix Γ in proposition 3. Second, they over-approximate the zonotope by a parallelotope, or by the intersection, or the Minkowski sum of parallelotopes respectively.

Method A The first method computes two different over-approximating parallelotopes Ψ_A and Ψ_{IH} of a zonotope Z. The first parallelotope $\Psi_A = \Gamma_A \cdot \mathcal{IH}(\Gamma_A^{-1} Z)$ is generated from the n longest generators of Z, i.e. $\Gamma_A = \left[g^{(i_1)}, \ldots, g^{(i_n)}\right]$ such that $\|g^{(i_1)}\|_2 \geq \ldots \geq \|g^{(i_p)}\|_2$. The second parallelotope $\Psi_{IH} = \mathcal{IH}(Z)$ is the interval hull of Z. The resulting over-approximating polytope P is computed as the intersection of both parallelotopes: $P = \Psi_A \cap \Psi_{IH}$.

Method B This method generates an over-approximating parallelotope Ψ_B of Z from the n generators in Γ_B that span the largest volume, i.e. $vol(\Gamma_B) \geq vol(\Gamma^*)$ for all $\Gamma^* = \left[g^{(i_1)}, \ldots, g^{(i_n)}\right]$ composed of n generators which are selected from the original p generators. The volume spanned by the n generators of Γ is well known to be computed as $vol(\Gamma) = \det(\Gamma)$. Note that the volumes have to be computed for all of the $p!/((p-n)!n!)$ possibilities of choosing n generators out of the p original generators.

Method C Method C is based on method B. Due to the factorial growth of the computational complexity of method B, method C applies method B on a subset of generators $g^{(1)}, \ldots, g^{(r)}$ with $n < r < p$. The subset of generators is determined by picking the r longest generators as presented in method A.

Method D Method D is based on method C. In order to increase the accuracy of method C, its resulting parallelotope Ψ_C is intersected with the interval hull of Z, denoted Ψ_{IH}: $P = \Psi_C \cap \Psi_{IH}$.

Method E This method reduces the order of the original zonotope to a zonotope of order 2 as presented in Girard [2005]. The reduction is performed by computing the interval hull of $p-n$ generators chosen such that $\|g^{(i_1)}\|_1 - \|g^{(i_1)}\|_\infty \leq \ldots \leq \|g^{(i_{q-n})}\|_1 - \|g^{(i_{q-n})}\|_\infty$. The resulting interval hull is denoted Ψ_{IH}^* and the parallelotope of the n remaining generators is denoted Ψ_E. Thus, the original zonotope is over-approximated by the Minkowski sum of Ψ_E and Ψ_{IH}^* ($Z \subseteq \Psi_E + \Psi_{IH}^*$). Note that Ψ_{IH}^* differs from Ψ_{IH} as it is computed from $p-n$ instead of p generators. The resulting polytope P is computed by the Minkowski sum of the halfspace representation of Ψ_E and Ψ_{IH}^*.

5.3 Evaluation of Reduction Methods

In order to evaluate the proposed methods, they are applied to 100 instances of randomly generated zonotopes. Each randomly obtained generator $g^{(i)}$ is composed by a

random vector $\hbar^{(i)}$ multiplied by a random variable $y^{(i)}$: $g^{(i)} = y^{(i)} \cdot \hbar^{(i)}$. The elements of $\hbar^{(i)}$ have a uniformly distributed probability density function within the interval $[-1, 1]$ and $y^{(i)}$ is uniformly distributed within the interval $[0, 1]$. Without loss of generality, the center of the zonotopes is chosen as the origin. The random variable $y^{(i)}$ is optional, but accounts for the observation that the generators of reachable sets usually have a significant diversity in length.

The proposed methods are evaluated in terms of the mean computation time t and the metric $\Theta = (vol(P)/vol(Z))^{1/n}$ where $vol()$ determines the volume of the original zonotope Z and its over-approximating polytope P. This metric determines the ratio of the edge length of two cubes, in which the volume of the polytope and the zonotope fit. Thus, this metric is independent of the dimension n if the over-approximation is equal for each dimension. The computational times are measured on a notebook dual core processor (1.66 GHz) and the reduction techniques are implemented in Matlab. The polytope operations, such as the Minkowski addition of polytopes for Method E are performed with the Matlab toolbox MPT (Kvasnica et al. [2004]). The number of pre-filtered generators for method C and D are chosen as $r = 2n$.
The results are shown in Tab. 1, and the best performing method is indicated by underlined results. For low dimensions, all methods have small computation times allowing to choose the most accurate method. For zonotopes of second order, method E is the best choice as it returns the exact result. For zonotopes of order 4, method E is outperformed by method D. The only methods that are capable of over-approximating zonotopes of order greater than 6 in reasonable time are method A, C and D. However, table 1 is limited to zonotopes of order 6 as the computation of volumes for high order zonotopes is infeasible, e.g. the volume of a zonotope of dimension 10 and order 4 has to be computed by the sum of the volumes of $8.5 \cdot 10^8$ parallelotopes. The mean computation times for high dimensional problems, e.g. for zonotopes of dimension 20 and order 4 are 1.56, 2.95 and 3.80 seconds for methods A,C and D respectively, if the number of pre-filtered generators of method C and D are $r = 24$.

Table 1. Results for Zonotope Reduction.

Meth.	mean of t [sec]:	mean of Θ:	[min,max] of Θ:	variance of Θ:
dimension $n = 2$, zonotope order $q = 2$, $\bar{t}_{exact} = 0.0131$				
A:	0.0156	1.0234	[1.0010, 1.1617]	0.0005
B:	0.0038	1.0463	[1.0005, 1.2544]	0.0016
C:	0.0033	1.0463	[1.0005, 1.2544]	0.0016
D:	0.0094	1.0230	[1.0005, 1.1026]	0.0005
E:	0.0131	1.0000	[1.0000, 1.0000]	0.0000
dimension $n = 2$, zonotope order $q = 4$, $\bar{t}_{exact} = 0.0360$				
A:	0.0166	1.0486	[1.0078, 1.1265]	0.0009
B:	0.0044	1.0809	[1.0196, 1.2668]	0.0017
C:	0.0034	1.1004	[1.0196, 1.5841]	0.0076
D:	0.0095	1.0345	[1.0054, 1.1106]	0.0004
E:	0.0135	1.1577	[1.0279, 1.4159]	0.0055
dimension $n = 4$, zonotope order $q = 2$, $\bar{t}_{exact} = 0.2766$				
A:	0.0222	1.2475	[1.0227, 1.5958]	0.0155
B:	0.0060	1.1688	[1.0233, 1.5061]	0.0059
C:	0.0058	1.1688	[1.0233, 1.5061]	0.0059
D:	0.0163	1.1391	[1.0227, 1.3177]	0.0028
E:	0.2766	1.0000	[1.0000, 1.0000]	0.0000
dimension $n = 4$, zonotope order $q = 4$, $\bar{t}_{exact} = 12.531$				
A:	0.0213	1.2987	[1.1563, 1.5057]	0.0047
B:	0.0879	1.2884	[1.1381, 1.6349]	0.0056
C:	0.0060	1.3220	[1.1381, 1.9406]	0.0155
D:	0.0163	1.2140	[1.1183, 1.3223]	0.0015
E:	0.2535	1.4298	[1.2968, 1.6489]	0.0038
dimension $n = 6$, zonotope order $q = 2$, $\bar{t}_{exact} > 10min$				
A:	0.0293	1.4708	[1.1590, 2.0263]	0.0441
B:	0.0203	1.2875	[1.0890, 1.5727]	0.0076
C:	0.0203	1.2875	[1.0890, 1.5727]	0.0076
D:	0.0367	1.2579	[1.0888, 1.4469]	0.0045
dimension $n = 6$, zonotope order $q = 4$, $\bar{t}_{exact} > 10min$				
A:	0.0903	1.5292	[1.3096, 1.7924]	0.0104
B:	98.320	1.4744	[1.3062, 1.6853]	0.0066
C:	0.0219	1.5218	[1.3062, 1.8538]	0.0110
D:	0.0391	1.3842	[1.2592, 1.4841]	0.0017

5.4 Over-Approximation of a Set of Polytopes

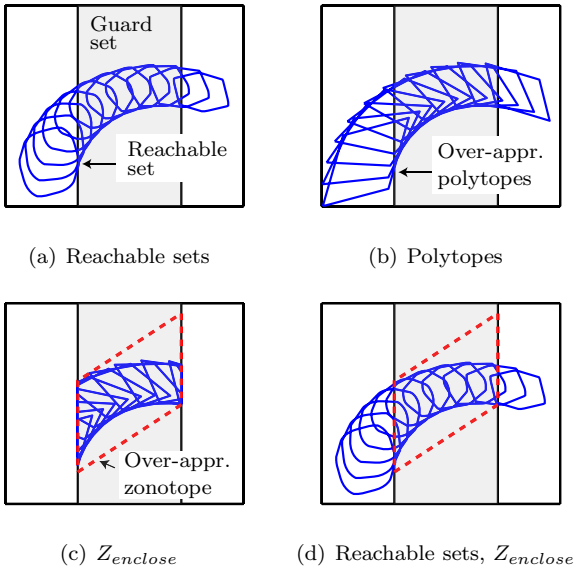
In order to continue the computation of reachable sets after their intersection with guards, they have to be over-approximated by zonotopes. The resulting polytopes from the intersection with a single guard set are denoted $P_1, \ldots, P_o$ (increasing index for increasing time interval) and their over-approximation is computed as follows:

(1) The polytopes P_1 and P_o of the first and last time interval intersecting the guard set are over-approximated by interval hulls $\mathcal{H}_1$ and $\mathcal{H}_2$. The interval hulls are obtained by computing the vertices of P_1, P_o and determining their minimum and maximum values for each dimension.
(2) The volumetric centers c_1 and c_2 of $\mathcal{H}_1$ and $\mathcal{H}_2$ are computed. The vector $l = (c_2 - c_1)/\|c_2 - c_1\|_2$ is introduced which approximates the direction, the reachable set is heading to.
(3) The vertices of $P_1, \ldots, P_o$ are unified in the matrix V of all vertices. The set of vertices is transformed by the inverse of a matrix Λ of unit vectors e_i aligned to the coordinate axis, where the unit vector that best correlates with l is replaced by l: $\Lambda = [\ldots, e_{i-1}, l, e_{i+1}, \ldots]$, $|e_i^T l| > |e_k^T l|$, $\forall k = 1 \ldots o$. The transformed set of vertices is $V_{trans} = \Lambda^{-1} V$.
(4) The enclosing zonotope is obtained analogously to proposition 3 by computation of the interval hull of V_{trans} and a transformation to the original coordinate system: $Z_{enclose} = \Lambda \cdot \mathcal{IH}(\Lambda^{-1} V)$.

The steps for the intersection of a reachable set with a guard set are illustrated exemplarily in Fig. 3. The reachable set represented by zonotopes and the guard set are shown in Fig. 3(a). In order to intersect the reachable sets with the guard set, the earlier are over-approximated by polytopes using method C, see Fig. 3(b). The intersected polytopes together with the enclosing zonotope $Z_{enclose}$ are presented in Fig. 3(c). A comparison of the original reachable set with the obtained over-approximating zonotope $Z_{enclose}$ is given in Fig. 3(d).

6. ROOM HEATING EXAMPLE

The presented techniques are applied to a benchmark example proposed by Fehnker and Ivančić [2004]: It considers 6 rooms with heaters in the rooms 1 and 6 (Fig. 4(a)). The heaters are switched on if the temperature drops below



(a) Reachable sets (b) Polytopes

(c) $Z_{enclose}$ (d) Reachable sets, $Z_{enclose}$

Fig. 3. Reachable sets intersected with guard set.

20 and switched off if the temperature exceeds 24. The temperature dynamics in room i is:

$$\dot{x}_i = c_i h_i + b_i(u - x_i) + \sum_{i \neq j} a_{ij}(x_j - x_i)$$

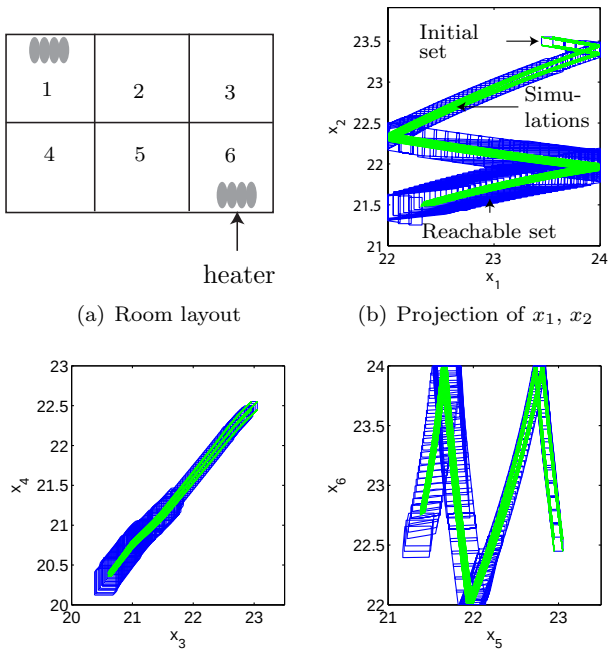
with constants a_{ij}, b_i and c_i. The rate of heat exchange a_{ij} between two adjacent rooms is 0.5. The transfer rate from inside the building to the outside is 0.16 for rooms at corners and 0.08 for other rooms. The outside temperature u is in the interval of $[0, 0.25]$ and $h = 15$ for both heaters. The reachable sets are computed for the time interval $t \in [0, 1]$ using Method D and visualized in Fig. 4. A possible verification scenario is to analyze whether a certain combination of room temperatures is enabled (or avoided) by the switching controller. The scenario is implemented in Matlab, and the computation time is 5.05 seconds on a notebook dual core processor (1.66 GHz).

7. CONCLUSION

The paper has proposed an approach to compute reachable sets of hybrid systems using zonotopes with special focus on the set computations required for transitions and resets. The main advantage of zonotopes is the efficient computation of continuous reachable sets in high dimensions. Additionally, the over-approximation of zonotopes by polytopes and the enclosure of polytopes by a single zonotope can be computed efficiently in high-dimensional spaces. The drawback of this method is, that the reachable set has to be over-approximated when intersecting with guard sets. However, algorithms that only use general convex polytopes throughout the procedure suffer from the same problem – this in addition to a much worse scaling of the reachable set computation with the dimension n and with the number of halfspaces.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge partial financial support by the German Research Foundation (DFG) within the Transregional Collaborative Research Centre 28 *Cognitive Automobiles*.



(a) Room layout (b) Projection of x_1, x_2

(c) Projection of x_3, x_4 (d) Projection of x_5, x_6

Fig. 4. Reachable sets of the room heating scenario.

REFERENCES

M. Althoff, O. Stursberg, and M. Buss. Reachability analysis of linear systems with uncertain parameters and inputs. In *Proc. 46th Conf. Decision and Control*, pages 726–732, 2007.

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

A. Chutinan and B. H. Krogh. Computational techniques for hybrid system verification. In *IEEE Transactions on Automatic Control*, volume 48, pages 64–75, 2003.

A. Fehnker and F. Ivančić. Benchmarks for hybrid systems verification. In *Hybrid Systems: Comp. and Control*, volume 2993 of *LNCS*, pages 326–341. Springer, 2004.

K. Fukuda. From the zonotope construction to the minkowski addition of convex polytopes. *Journal of Symbolic Computation*, 38(4):1261–1272, October 2004.

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

M. Kvasnica, P. Grieder, and M. Baotić. Multi-Parametric Toolbox (MPT), 2004. URL `http://control.ee.ethz.ch/~mpt/`.

D. Mortari. The n-dimensional cross product and its application to the matrix eigenanalysis. In *Proc. of the AIAA/AAS Astrodynamics Conference*, 1996.

O. Stursberg and B. H. Krogh. Efficient representation and computation of reachable sets for hybrid systems. In *Hybrid Systems: Comp. and Control*, volume 2623 of *LNCS*, pages 482–497. Springer, 2003.

G. M. Ziegler. *Lectures on Polytopes*. Graduate Texts in Mathematics. Springer-Verlag, 1995.