Proceedings of the
44th IEEE Conference on Decision and Control, and
the European Control Conference 2005
Seville, Spain, December 12-15, 2005



# Reachability Analysis for Affine Systems Using $\epsilon$-Decomposition

Zhi Han and Bruce H. Krogh

***Abstract*— This paper presents an approach to compute conservative approximations to the set of reachable states and outputs for affine systems using $\epsilon$-decomposition techniques. Instead of performing reachability analysis on the full-order system model, the method presented in this paper first applies $\epsilon$-decomposition to obtain a number of $\epsilon$-coupled subsystem models, and then performs reachability analysis on the subsystems, thus avoiding the complexity involved in computing reach sets for high-order system models. The approach is illustrated with numerical examples.**

## I. Introduction

Recently there has been considerable interest in applying formal verification techniques to continuous and hybrid dynamical systems [1], [2]. The main obstacle in applying verification techniques to engineering applications is the complexity of *reachability analysis*, that is, the representation and computation of the sets of reachable states for models of continuous dynamic systems. Current verification tools can handle systems with only a few (less than 10) continuous state variables, which limits the value of their use for many real systems [3]. As a result, the verification of continuous and hybrid systems needs to be performed on reduced-order models [4], [5], or on subsystems of the full model [6], [7]. This paper presents an approach to compute the reach sets for affine dynamic systems based on the analysis of $\epsilon$-coupled subsystems [8].

$\epsilon$-decomposition, which has been used in connective stability analysis [9] and near-optimal controller synthesis [10], makes it possible to extend current methods of reachability analysis to larger system models. The full-order system model is decomposed into $\epsilon$-coupled subsystems and reachability analysis is performed for the decoupled subsystems corresponding to $\epsilon = 0$. These reach sets are then augmented to account for the approximation error introduced by neglecting the $\epsilon$-coupling, leading to conservative over-approximations of the reach sets for the full-order system model. To reduce the approximation error, we present a method to compute the reach set based on an asymptotic expansion of the system trajectories with respect to the decoupling factor $\epsilon$ [11]. We show that under certain conditions the approximation error can be made arbitrarily small.

## II. Preliminaries

A linear time-invariant system is described by

$$\dot{x} = Ax + Bu,\ y = Cx. \tag{1}$$

Z. Han and B. H. Krogh are with Department of Electrical and Computer Engineering, Carnegie Mellon University, 5000 Forbes Ave., Pittsburgh, PA 15213. Email: {zhih|krogh}@ece.cmu.edu

where $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times p}$, $C \in \mathbb{R}^{m\times n}$, $x(t) \in \mathbb{R}^n$ is a vector of state variables, $u(t) \in \mathbb{R}^p$ is a vector of input variables, and $y(t) \in \mathbb{R}^m$ is a vector of output variables. The norm $\|\cdot\|$ of vectors denotes the infinity norm, i.e., $\|x\| = \max_{1\le i\le n} |x_i|$. $\mathcal{L}_\infty[t_0, t_f]$ denotes the normed space consisting of Lebesgue measurable functions $x(t)$ defined on interval $[t_0, t_f] \subseteq \mathbb{R}$ with the $\mathcal{L}_\infty$ norm given by $\|x(\cdot)\|_{\mathcal{L}_\infty[t_0,t_f]} \equiv \sup_{t\in[t_0,t_f]} \|x(t)\| < \infty$.

*Theorem 1 ([12]):* For LTI system (1), with $x(t_0) = 0$, the $\mathcal{L}_\infty[t_0, t_f]$ induced norm of the system for the time interval $[t_0, t_f]$, where $t_0 \le t_f$, is given by

$$G_\infty(A, B, C) \equiv \sup_{u\in\mathcal{L}_\infty} \frac{\|y\|_{\mathcal{L}_\infty}}{\|u\|_{\mathcal{L}_\infty}} = \int_0^{t-t_0} \|Ce^{A\tau}B\| d\tau \tag{2}$$

This paper concerns reachability analysis of affine dynamic systems of the form

$$\mathcal{S}(A, b, C):\ \begin{array}{l} \dot{x}(t) = Ax(t) + b \\ y(t) = Cx(t) \end{array} \tag{3}$$

For a given *initial condition* $(X_0, t_0)$, where $X_0 \subseteq \mathbb{R}^n$ is a closed set of initial states and $t_0 \in \mathbb{R}$ is the initial time, the *reach set* of an affine system (3) at time $t$ is defined as

$$Reach(\mathcal{S}, X_0, t_0, t) = \{x(t) | x(t) = e^{A(t-t_0)}x_0 + \int_{t_0}^{t} e^{A(t-\tau)}b d\tau, x(t_0) \in X_0\}.$$

The reach set of system $\mathcal{S}$ with initial condition $(X_0, t_0)$ over a time interval $[t_s, t_f]$ is defined as

$$Reach^{(o)}(\mathcal{S}, X_0, t_0, [t_s, t_f]) = \bigcup_{t\in[t_s,t_f]} Reach^{(o)}(\mathcal{S}, X_0, t_0, t)$$

where $t_0 \le t_s \le t_f < \infty$.

The *affine transformation* of a set $X \subset \mathbb{R}^n$ determined by a given matrix $A \in \mathbb{R}^{n'\times n}$ and vector $b \in \mathbb{R}^{n'}$ is denoted by $AX+b \equiv \{x' | x' = Ax+b,\ x \in X\} \subseteq \mathbb{R}^{n'}$. Thus, the *output reach set* of a system is given by $Reach^o(\mathcal{S}, X_0, t_0, t) = CReach(\mathcal{S}, X_0, t_0, t)$.

The reach set $Reach(\mathcal{S}, X_0, t_0, [t_0, t_f])$ can be represented approximately using a finite number of convex polytopes [13]. The procedure is outlined as follows. First the time interval $[t_0, t_f]$ is divided into $N$ equally spaced time segments, $[t_0, t_1]$,$[t_1, t_2]$,...,$[t_{N-1}, t_N]$. Polytopic approximation of the reach set $Reach(\mathcal{S}, X_0, t_0, [t_{k-1}, t_k])$ is computed for each time segment $k$, which is denoted by $\hat{\mathcal{R}}^k$. The computed polytopes are over-approximations of the reach sets for each of the time segments, i.e., $Reach(\mathcal{S}, X_0, t_0, [t_{k-1}, t_k]) \subseteq \hat{\mathcal{R}}^k$. The complete reach set for $[t_0, t_f]$ is thus the union of $N$ segments $\hat{\mathcal{R}} = \bigcup_{k=1,\ldots,N} \hat{\mathcal{R}}^k$. For affine dynamic systems, the computation of the reach set segments consists of the following three steps [13]:

0-7803-9568-9/05/$20.00 ©2005 IEEE

1) (*Time Discretization*) Let $\Delta = (t_f - t_0)/N$ be the length of the time segments. Compute state transition matrix $\Phi = e^{A\Delta}$ and displacement $\Gamma = e^{A\Delta}\int_0^\Delta e^{-A\tau}bd\tau$.
2) (*Initial Segment Computation*) Compute $\hat{\mathcal{R}}^1$, an over-approximation of the reach set $Reach(\mathcal{S}, X_0, t_0, [t_0, t_0 + \Delta])$ for the first time segment.
3) (*Segments Evolution*) Compute all the remaining segments iteratively using the discrete-time formula $\hat{\mathcal{R}}^{k+1} = \Phi\hat{\mathcal{R}}^k + \Gamma$, $k = 1, \ldots, N-1$.

The over-approximation of the initial segment is represented using a convex polytope of the form $\mathcal{P}(\Pi, d) = \{x|\Pi x \leq d\} \subset \mathbb{R}^n$ where $\Pi \in \mathbb{R}^{p\times n}$ and $d \in \mathbb{R}^p$. The remaining reach set segments are computed as affine transformations of the initial segment. In this paper, each segment is represented by an *affine representation* $\mathcal{AP}(T, v, P) \subset \mathbb{R}^n$ of the set $\{x|x = Ty + v,\ y \in P = \mathcal{P}(\Pi, d) \subset \mathbb{R}^n\}$, where $T \in \mathbb{R}^{n\times n}$ is a linear transformation matrix, $v \in \mathbb{R}^n$ is a displacement vector and $P \subseteq \mathbb{R}^n$ is a polytope. An affine transformation of the set can be computed using $T$ and $v$ only, by which explicit operations on $P$ are avoided [14]. The affine representation was introduced in the context of affine arithmetic to preserve the linear correlations between uncertain variables in the computation of intervals [15]. If for a given polytope $P$, a set $X$ is represented by $\mathcal{AP}(T, v, P)$, then the affine transformation $AX + b$ can be represented by $\mathcal{AP}(AT, Av + b, P)$.

Next we introduce the $\epsilon$-decomposition for affine systems. Suppose that for some $\epsilon > 0$, the system matrix $A$ can be written as

$$A = A_D + \epsilon A_C \text{ where } A_C \in \mathbb{R}^{n\times n}$$
$$\text{and } A_D = \begin{bmatrix} A_{D1} & & \\ & \ddots & \\ & & A_{DM} \end{bmatrix} \text{ is block diagonal.} \quad (4)$$

The system $\mathcal{S}_D(A_D, b, C)$ with state vector $x_D \in \mathbb{R}^n$ is said to be an $\epsilon$-decomposition of $\mathcal{S}$. Analysis of the original full-order system $\mathcal{S}(A, b, C)$ can be performed on its decomposed approximation $\mathcal{S}(A_D, b, C)$ under some assumptions on $\epsilon$ [8], [9].

The state variables of the $\epsilon$-coupled affine systems are divided into $M$ subsystems according to the block partition of $A_D$, with the variables of the subsystems denoted as $x_{D1}, \ldots, x_{DM}$. The dynamics of the isolated subsystem $i$ is given as

$$\mathcal{S}_{Di} : \dot{x}_{Di}(t) = A_{Di}x_{Di}(t) + b_i \quad (5)$$

$i = 1, \ldots, M$. The system is thus decomposed into $M$ isolated subsystem models, which have lower-order state spaces than the original full-order system model. The approximation error is defined as $z_D(t) \equiv x(t) - x_D(t)$, $\forall t \in [t_0, t_f]$.

## III. Reachability Analysis Using Decomposition

The proposed decomposition-based reachability analysis procedure for affine dynamic systems is shown in Fig. 1. The procedure starts by decomposing the system using the $\epsilon-$decomposition technique. Reachability computation is then performed for each isolated subsystem. The results of all isolated subsystems are combined to estimate the approximation error $z_D$. The error bound is incorporated in the results to obtain conservative over-approximations of the reach sets for the full-order model. If the estimated error bound is too large, the procedure continues to compute more accurate reach sets using a higher-order asymptotic expansion of the decomposed subsystem. The order of expansion, $K$, is computed from estimation of bounds of the approximation error. The bounds of approximation error are incorporated into the final result to preserve conservativeness.

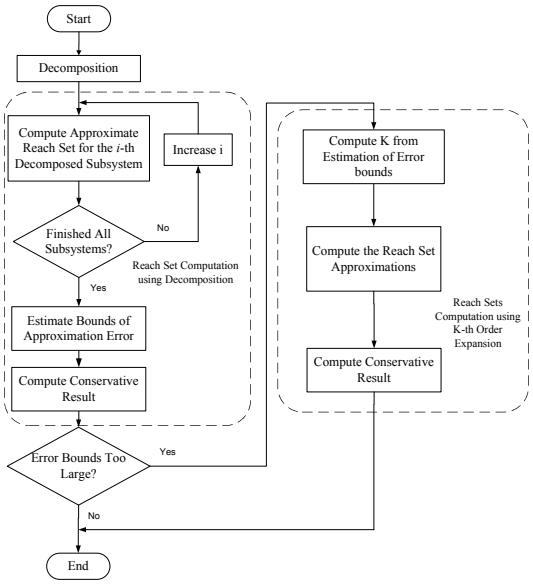



Fig. 1. Computation procedure.

This section discusses the first part of the procedure: the conservative reach set computation using decomposition. Observe that the isolated subsystems (5) are affine systems, for which the three-step procedure for reachability analysis presented in section II can be applied. The only remaining question is to estimate the bound on the error $z_D$ caused by $\epsilon$-decomposition.

For the original affine system $\mathcal{S}(A, b, C)$, denote the solution of system $\mathcal{S}$ for initial condition $(x_0, t_0)$ by $x(t) = x_D(t) + z_D(t)$, $t \in [t_0, t_f]$, where $z_D \in \mathbb{R}^n$ is the vector of approximation error. The system dynamics equation (3) is rewritten as [11]:

$$\frac{d}{dt}(x_D + z_D) = (A_D + \epsilon A_C)(x_D + z_D) + b.$$

Expanding the two sides of the equation, we have the differential algebraic equation involving both $x_D$ and $z_D$:

$$\begin{aligned} &\dot{x}_D + \dot{z}_D = A_D x_D + b + (A_D + \epsilon A_C)z_D + \epsilon A_C x_D \\ &x_D(t_0) + z_D(t_0) = x_0 \end{aligned} \quad (6)$$

where $x_D$ is the solution to the decomposed system

$$\dot{x}_D = A_D x_D + b \quad x_D(t_0) = x_0 \quad (7)$$

Subtracting (7) from (6), the resulting dynamic equation for $z_D$ is written as

$$\dot{z}_D = (A_D + \epsilon A_C) z_D + \epsilon A_C x_D \quad z_D(t_0) = 0 \tag{8}$$

Equation (8) gives the unique solution to the approximation error $z_D$ caused by the decomposition. The initial condition for $z_D$ is zero and the dynamics of $z_D$ is driven by the input signal $x_D$ scaled by $\epsilon$. Let the reach set of the variables $x_D$ and $z_D$ be $Reach_{x_D}(t)$ and $Reach_{z_D}(t)$, respectively. The output reach set of the original system $Reach^o(t) = \{y | y = Cx_D(t) + Cz_D(t), x \in Reach_{x_D}(t)$ and $z_D \in Reach_{z_D}(t)\}$ satisfies $Reach^o(t) \subseteq CReach_{x_D}(t) \oplus CReach_{z_D}(t)$, where $\oplus$ is the Minkowski sum operator.

We over-approximate the reach set $CReach_{z_D}(t)$ by a hyper-box $B_{\omega_D} = \{y | \|y\| \leq \omega_D, y \in \mathbb{R}^m\}$, where the radius of the box is estimated from $\|Cz_D(t)\|$. To estimate an upper-bound on $\|Cz_D(t)\|, t \in [t_0, t_f]$, let $y_e = Cz_D$ and $u = \epsilon x_D$. The dynamic equation (8) is rewritten as a linear dynamic system $\begin{cases} \dot{z}_D = Az_D + A_C u \\ y_e = Cz_D \end{cases}$ and $z_D(t_0) = 0$. The norm of the outputs $y$ can be estimated from the norm of the inputs $u$ and the induced norm of the linear dynamic system $G_\infty(A, A_C, C)$ using Theorem 1. The induced $\mathcal{L}_\infty$ norm of the linear system can be computed from a simulation run of its response $Ce^{At}A_C$. Although the original system might be large in size for reachability analysis, efficient simulation methods for large-scale linear systems have been studied extensively and there are algorithms and efficient software tools available to perform the simulation.

Since $\|Cz_D\|_{\mathcal{L}_\infty[t_0,t_f]} \leq \epsilon G_\infty(A, A_C, C)\ \|x_D\|_{\mathcal{L}_\infty[t_0,t_f]} = \omega_D$, the conservative over-approximation of reach set is computed as

$$\hat{\mathcal{R}}^k = C\hat{\mathcal{R}}^k_D \oplus B_{\omega_D} \tag{9}$$

for all the time segments $k$, where $\hat{\mathcal{R}}^k_D = \hat{\mathcal{R}}^k_{x_{D1}} \times \hat{\mathcal{R}}^k_{x_{D2}} \times \ldots \times \hat{\mathcal{R}}^k_{x_{DM}}$ is the cartesian product of the conservative reach sets computed for the subsystems. To compute the output reach set of subsystem $i$, $\mathcal{R}^k_{x_{Di}}$ is projected to the output space as $C_i\mathcal{R}^k_{x_{Di}}$ where $C_i$ is a sub-matrix of $C$ corresponding to subsystem $i$. $\hat{\mathcal{R}}^k$ is then computed as $\oplus_{i=1}^M C_i\mathcal{R}^k_{x_{Di}} \oplus B_{\omega_D}$. If exact computation of the Minkowski sum is too complex, over-approximation methods such as the ORH [16] or face-lifting [17] may be used to compute $\hat{\mathcal{R}}^k$.

## IV. Computing Reach Sets for $K^{th}$-Order Expansion

The previous section presents an approach based on $\epsilon$-decomposition to over-approximate reach sets for $\epsilon$-coupled affine systems. The reachability analysis result is the Minkowski sum of $CReach_{x_D}$ and $B_\omega$. Since the error bound estimate $\omega$ is proportional to $\|x_D\|_{\mathcal{L}_\infty[t_0,t_f]}$, the approximation could be too conservative if $\|x_D\|_{\mathcal{L}_\infty[t_0,t_f]}$ is not small. This section presents an approach to compute the reach sets based on the asymptotic expansion of the state trajectories with respect to $\epsilon$. It is shown in the next section that using an affine polytope computation, the approximate reach set can be computed to be arbitrarily close to the reach set of the full-order system.

The following proposition provides an iterative approach to approximate the trajectory of an $\epsilon$-coupled affine dynamic system with the trajectories of systems generating the approximation errors.

*Proposition 1 (Asymptotic Expansion):* Consider the affine dynamic system modeled by

$$\dot{x} = (A_D + \epsilon A_C)x + Bu,\ x(t_0) = x_0$$

where $\epsilon > 0$. The solution of the linear dynamic system can be written as

$$x(t) = x_{(0)}(t) + x_{(1)}(t) + \cdots + x_{(K)}(t) + z_K(t)$$

where $x_{(K)}$ and $z_K$ satisfies

$$\begin{array}{ll} \dot{x}_{(0)} = A_D x_{(0)} + b & x_{(0)}(t_0) = x_0 \\ \dot{x}_{(1)} = A_D x_{(1)} + \epsilon A_C x_{(0)} & x_{(1)}(t_0) = 0 \\ \vdots & \vdots \\ \dot{x}_{(K)} = A_D x_{(K)} + \epsilon A_C x_{(K-1)} & x_{(K)}(t_0) = 0 \\ \dot{z}_K = (A_D + \epsilon A_C) z_K + \epsilon A_C x_{(K)} & z_K = 0 \end{array}$$

*Proof:* Let $x(t) = x_{(0)}(t) + x_{(1)}(t) + \ldots + x_{(K)}(t) + z_K(t),\ t \in [t_0, t_f]$, replace the $x$ in the system equation (3). The dynamic equations for $x_{(0)}, \ldots, x_{(K)}, z_K$ are obtained by inductively equating both sides of the equation. Since the system is an affine system, the solution to the set of differential equations exists and is unique. ■

Since $x_{(0)} = x_D$ in (7), the zeroth-order approximation is exactly the same as the isolated subsystems. Proposition 1 suggests a sequential way to compute approximations to reach sets for $x_{(1)}$, ..., $x_{(K)}$. For any $l \leq K$, since $x_{(l)}$ depends only on $x_{(0)}$, ..., $x_{(l-1)}$, the reach set of $x_{(l)}$ can be computed from the previous results on reach sets of $x_{(0)}$ ..., $x_{(l-1)}$. Proposition 1 also introduces a method to reduce the approximation error $z_K$ by increasing the expansion order $K$. Indeed, we have the following proposition.

*Proposition 2 (Bounds for $K^{th}$-Order Approximation):* For the $K^{th}$-order approximation system model, we have $\|Cz_K\|_{\mathcal{L}_\infty[t_0,t_f]} \leq \epsilon^{K+1} G^K_\infty(A_D, A_C, I)\ G_\infty(A, A_C, C)\ \|x_D\|_{\mathcal{L}_\infty[t_0,t_f]}$, where $I_{n\times n}$ is the $n^{th}$-order identity matrix.

*Proof:* Proof by induction on $K$. For K=0, the bound is true since $z_0 = z_D$.

Assume the bound is valid for $K-1$. For the $K^{th}$ expansion, the solution of $x_{(K)}$ is $x_{(K)}(t) = \int_{\tau=t_0}^{t} e^{A_D(t-\tau)}\ \epsilon A_C x_{K-1}(\tau) d\tau$, therefore $\|x_{(K)}\|_{\mathcal{L}_\infty[t_0,t_f]} \leq \epsilon G_\infty(A_D, A_C, I)\|x_{(K-1)}\|_{\mathcal{L}_\infty[t_0,t_f]}$. Then $\|Cz_K\| \leq \epsilon G_\infty(A, A_C, C)\ \|x_{(K)}\|_{\mathcal{L}_\infty[t_0,t_f]} \leq \epsilon^{K+1} G^K_\infty(A_D, A_C, I)\ G_\infty(A, A_C, C)\ \|x_D\|_{\mathcal{L}_\infty[t_0,t_f]}$. ■

If $\epsilon < 1/G_\infty(A_C, A_D, I)$, we say that the $\epsilon$-coupled subsystems $\mathcal{S}_1, \ldots, \mathcal{S}_M$ are *weakly-coupled*. For reachability analysis of a number of weakly-coupled subsystems, the necessary approximation order $K$ can be estimated before the reach sets of $x_{(1)}$, ..., $x_{(K)}$ are computed. Let $\omega_{tol}$ denote the selected tolerance for approximation error such that $\|Cz_K\| \leq \omega_{tol}$. From Proposition 2 the expansion order

$K$ is estimated as $K = ceil(\frac{|\log(\omega_{tol}/\epsilon G_\infty(A,A_C,C))}{|\log(\epsilon G_\infty(A_C,A_D,I))|})$. The application context will determine an appropriate value for $\omega_{tol}$.

To perform computation of the reach sets for the $K^{th}$-order expansion, suppose we have obtained conservative results for $Reach_{x_{(0)}}$. Let $\bar{x}(K) = \begin{bmatrix} x_{(0)} & \dots & x_{(k)} \end{bmatrix}^T$ be the augmented vector of state variables of equation (1). The $K^{th}$-order approximate model can be written as

$$\dot{\bar{x}} = \bar{A}\bar{x} + \bar{b},\ y = \bar{C}\bar{x}$$

The system matrix $\bar{A}$ for the augmented state has the following special structure where only the diagonal and subdiagonal blocks are nonzero:

$$\bar{A}_{(K+1)n\times(K+1)n} = \begin{bmatrix} A_D & 0 & \dots & \dots & 0 \\ \epsilon A_C & A_D & 0 & \dots & 0 \\ & \ddots & \ddots & \ddots & \\ 0 & 0 & \epsilon A_C & A_D & 0 \\ 0 & 0 & \dots & \epsilon A_C & A_D \end{bmatrix}$$
$$\bar{b}_{(K+1)n\times 1} = \begin{bmatrix} b^T & 0 & 0 & \dots & 0 \end{bmatrix}^T$$
$$\bar{C}_{p\times(K+1)n} = \begin{bmatrix} C & C & \dots & C \end{bmatrix}$$

The $K^{th}$-order approximation reach set for $Reach^o$ is computed using the following procedure. We use the subscript $(l)$ in parenthesis to denote the current step of expansion $l$ and the subscript $i$ to denote that the reach set is computed for the $i^{th}$ decomposed subsystem.

1) *(Time Discretization)* Let $\Delta = (t_f - t_0)/N$ be the length of each time segment. Compute the state transition matrix $\Phi = e^{\bar{A}\Delta}$. Notice that the system matrix $\bar{A}$ is lower block-triangular, thus the discrete-time state transition matrix is lower-block-triangular.

$$\bar{\Phi}_{(K)} = \begin{bmatrix} \Phi_D & & & \\ \Phi_{(10)} & \Phi_D & & \\ \vdots & \vdots & \ddots & \\ \Phi_{(K0)} & \Phi_{(K1)} & \dots & \Phi_D \end{bmatrix}$$

Since we are computing the reach set for the $K^{th}$-order expansion, only the $K^{th}$ row of matrix $\Phi$ is required. Partition each block $\Phi_{(lj)}$, $0 \le j < l \le K$ as $\begin{bmatrix} \Phi_{(lj)11} & \dots & \Phi_{(lj)1M} \\ \vdots & \vdots & \vdots \\ \Phi_{(lj)M1} & \dots & \Phi_{(lj)MM} \end{bmatrix}$ according to the decomposition of $A_D$.

2) *(Initial Segment Approximation)* For $i = 0, \dots, M$ and $l = 1, \dots, K$, compute the reach set approximation $\hat{\mathcal{R}}^1_{(l)i}$ for the initial segment $[t_0, t_0 + \Delta]$ and all subsystems $i$ in expansions $l$.
3) *(Evolution)* Evolve the reach sets for the subsystems $i$ for expansion $l$ using the discrete-time dynamics $\hat{\mathcal{R}}^{k+1}_{(l)i} = \Phi_D\hat{\mathcal{R}}^k_{(l)i} + \sum_{j=0}^{l-1}\sum_{q=1}^{M}\Phi_{(lj)iq}\hat{\mathcal{R}}^k_{(j)q}$.
4) *(Error Estimation)* Compute $\omega_K = \|Cz_k\|_{\mathcal{L}_\infty[t_0,t_f]}$ using Proposition 2.
5) *(Output Projection)* Compute the $K^{th}$-order approximate output reach set as $\hat{\mathcal{R}}^o = \sum_{l=0}^{K} C\hat{\mathcal{R}}_{(l)} \oplus B_{\omega_K}$

For the $l^{th}$ expansion, the $i^{th}$ subsystem is under consideration. The dynamic equation for $x_{(l)i}$ is

$$\mathcal{S}_{(l)i}: \begin{array}{l} \dot{x}_{(l)i} = A_{Di}x_{(l)i} + A_{Ci}x_{(l-1)} \\ x_{(l)i} = 0 \end{array}$$

To compute the reach set for $[t_0, t_0 + \Delta]$, we compute a polytopic over-approximation of $Reach(\mathcal{S}_{(l)i},\ 0,\ w(\cdot),[t_0, t_0 + \Delta])$ for uncertain input signal $w(t) \in U = \hat{\mathcal{R}}_{(l-1)1} \times \hat{\mathcal{R}}_{(l-1)2} \times \dots \hat{\mathcal{R}}_{(l-1)M}, \forall t \in [t_0, t_0 + \Delta]$, where $\hat{\mathcal{R}}_{(l-1)1}, \dots, \hat{\mathcal{R}}_{(l-1)M}$ are the reach sets for the subsystems computed for the $(l-1)^{th}$ expansion. The result is an over-approximation of the reach set of the system. Let $\Pi_j \in \mathbb{R}^n$ be the unit vector denoting the outward direction of a facet of a polytope. A polytopic over-approximation of the reach set for $[t_0, t_0+\Delta]$ with bounded uncertain input is computed as the optimal solution to the following problem for all the facets $\Pi_j$ of the polytope.

$$\begin{array}{ll} & max_{u,t}\Pi_j^T\tilde{x}_i(t) \\ s.t. & \dot{\tilde{x}}_i(t) = A_{Di}\tilde{x}_i(t) + A_{Ci}w(t),\ \tilde{x}_i(t_0) = 0 \\ & w(t) \in U \text{ and } t \in [t_0, t_0 + \Delta] \end{array} \quad (10)$$

Notice that the solution to the linear system with zero initial condition has closed-form $\tilde{x}_i(t) = \int_0^t e^{A_{Di}(t-s)}A_{Ci}u(s)dt$. For a fixed $t$, the optimal control input is [18]:

$$u(s) \in \arg\max\{\Pi_j^T e^{A_{Di}(t-s)}A_{Ci}u(s) | u(s) \in U\}$$

and the optimal cost is

$$\begin{aligned} max_u\Pi_j^T\tilde{x}_i(t) &= \int_0^t \Pi_j^T e^{A_{Di}(t-s)}A_{Ci}u^*(s)ds \\ &= \int_0^t max_{u\in U}\Pi_j^T e^{A_{Di}(t-s)}A_{Ci}uds \\ &= \int_0^t max_{u\in U}\Pi_j^T e^{A_{Di}\tau}A_{Ci}ud\tau \end{aligned} \quad (11)$$

Let $d_j^*(t) = \max_u \Pi_j^T\tilde{x}_i(t)$ be the optimal solution to (11) for any time $t \in [t_0, t_0+\Delta]$. The solution to (10) for the time segment is then the maximum of $d_j = \max_{t\in[t_0,t_0+\Delta]} d_j^*(t)$. For computation, we choose $\Pi_{(l)i} = \Pi_{(l-1)i}$. The computation of $d_j^*$ can be carried out by solving the ODE (11) for the trajectory and then $d_j$ is obtained from the peak value of $d_j^*(t)$ such that $\Pi_j\tilde{x}_i(t) \le d_j$, $t \in [t_0, t_0 + \Delta]$.

With the affine representation, the reach set segments are evolved using affine transformations of the initial segments. For the $K^{th}$-order expansion and the $i^{th}$ subsystem, notice that the discrete-time system transition matrix $\bar{\Phi}_{(K)}$ is lower-block triangular, the reach set for the subsystem $i$ is an affine transformation of the initial segments of zeroth to $(K-1)^{th}$ expansions of all subsystems and the initial segment of the $K^{th}$ expansion of the $i^{th}$ subsystem, i.e., $P = \mathcal{R}^1_{(0)} \times \mathcal{R}^1_{(1)} \times \dots \times \mathcal{R}^1_{(K-1)} \times \mathcal{R}^1_{(K)i}$. Therefore the size of the transformation matrix $T_{(K)i}$ can be as large as $n_i \times (nK+n_i)$. As the order of expansion $K$ increases, computational complexity increases polynomially for the affine transformation step. Since the computation is performed on subsystems, the representation and computation of reach sets in the full-order state space is avoided.

## V. Error Analysis

This section presents bounds on the over-approximation error of the reach set computation. We neglect the error caused by numerical computation and only consider the over-approximation errors in the representation. Observe that Step 3 in the procedure applies the affine transformation only to the initial segments, which does not introduce any extra approximation errors using the affine representation. The only sources of errors are from the initial segments and the decomposition. We show that the error in terms of Hausdorff distance between the actual reach set and the approximation computed using decomposition can be made arbitrarily small. The Hausdorff distance for two sets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{R}^n$ is defined as $dist(\mathcal{U}, \mathcal{V}) = \inf\{\omega | U \subset V \oplus B_\omega \text{ and } V \subseteq U \oplus B_\omega\}$. In the following discussion we consider the augmented system $\bar{\mathcal{S}}(\bar{A}, \bar{b}, \bar{C})$ for the $K^{th}$-order approximation. Further we assume that the initial condition $(X_0, t_0)$ is given as $X_0 = X_{01} \times X_{02} \times \ldots \times X_{0M}$, i.e., the initial states of the subsystems are given independently.

*Proposition 3 (Errors in Initial Segments):* For any expansion $l$ and subsystem $i$, let $\hat{\mathcal{R}}^1_{(l)i}$ denote the over-approximation of reach set in terms of $x_{(l)i}$ for the first segment $[t_0, t_0 + \Delta]$ . For any given $\omega > 0$ there exists a $\Delta$ such that $dist[\hat{\mathcal{R}}^1_{(l)i}, Reach_{x_{(l)i}}(\bar{\mathcal{S}}, \bar{X}_0, t_0, [t_0, t_0 + \Delta])] < \omega$.

*Proof:* Observe the fact that $\bar{X}_{(l)i}(t_0) \subseteq Reach_{x_{(l)i}}(\bar{\mathcal{S}}_D, \bar{X}_0, t_0, [t_0, t_0 + \Delta])$. We prove the proposition by proving that there exists a $\Delta$ such that $dist(\hat{\mathcal{R}}^1_{(l)i}(\Delta), X_{(l)i}(t_0)) < \omega$. For $l = 0$ the computation of $\hat{\mathcal{R}}^1$ is exactly the same as that of [13] since the $X_{0i}$ are given individually. Thus the segment approximation can be made arbitrarily close to $X_{(0)i}(t_0)$, i.e., $dist(\mathcal{R}^1_{(0)i}, X_{0i}) < \omega$.

For $l > 0$ the initial state of $x_{(l)i} = 0$. The objective then is to prove the reach set can be bounded by a small hyper-box $B_\omega$, that is equivalent to $\|\hat{\mathcal{R}}^1_{(l)i}\| \equiv \sup_{x_{(l)i} \in \hat{\mathcal{R}}^1_{(l)i}} ||x_{(l)i}|| < \omega$.

Indeed, since each facet of $\hat{\mathcal{R}}^1_{(l)i}$ is computed by finding the peak value of the optimal trajectory of (11), we have

$$\begin{aligned}
& \max_{t \in [t_0, t_0+\Delta]} \max_u \Pi_i^T x_{(l)i}(t) \\
= & \max_{t \in [t_0, t_0+\Delta]} \int_0^t \max_{u \in U} \Pi_i^T e^{A_{Di}\tau} A_{Ci} u d\tau \\
\leq & |\Pi_i| \int_0^\Delta e^{|A_{Di}|\tau} |A_{Ci}| d\tau \sup_{u \in U} |U| \\
\leq & \Delta |\Pi_i| e^{|A_{Di}|\tau} |A_{Ci}| \sup_{u \in U} |U| \\
= & \Delta |\Pi_i| M \sup_{u \in U} |U|
\end{aligned}$$

Since $\Pi_i$ is a unit vector, $M$ depends only on the system matrices $A_D$ and $A_C$, and $U = \hat{\mathcal{R}}^1_{(0)} \times \hat{\mathcal{R}}^1_{(1)} \times \ldots \hat{\mathcal{R}}^1_{(l-1)}$ is bounded. For any expansion $l$, we can always choose a small enough $\Delta$ such that $\|\hat{\mathcal{R}}^1_{(l)i}\| \leq \omega$. ∎

A corollary of Proposition 3 is that the error of the reach set computed for $[t_0, t_f]$ for the $l^{th}$ order approximate model can be made arbitrarily small.

*Corollary 1:* For any expansion $l$ and subsystem $i$, let $\hat{\mathcal{R}}_{(l)i} = \bigcup_{k=1,\ldots,N} \hat{\mathcal{R}}^k_{(l)i}$ denote the over-approximation of reach set in terms of $x_{(l)i}$ for $[t_0, t_f]$ . For any given $\omega > 0$ there exists a $\Delta$ such that $dist[\hat{\mathcal{R}}_{(l)i}, Reach_{x_{(l)i}}(\bar{\mathcal{S}}, \bar{X}_0, t_0, [t_0, t_f])] < \omega$.

*Proof:* Apply Proposition 3 to $\omega' = e^{-|\bar{A}|(t_f - t_0)}\omega$. The proposition then follows from

$$dist[\hat{\mathcal{R}}_{(l)i}, Reach_{(l)i}(\bar{\mathcal{S}}, \bar{X}_0, t_0, [t_0, t_f])] \leq e^{|\bar{A}|(t_f - t_0)} dist[\hat{\mathcal{R}}^1_{(l)i}, Reach_{x_{(l)i}}(\bar{\mathcal{S}}, \bar{X}_0, t_0, [t_0, t_0 + \Delta])] < \omega$$

∎

We conclude this section with the following proposition, which claims that when $\epsilon$ is bounded, the reach set computed using the iterative procedure can be made arbitrarily close to the actual reach set of the full-order system model.

*Proposition 4:* Assume $\epsilon G_\infty(A_D, A_C, I) < 1$, let the reach set computed using $K^{th}$-order asymptotic expansion be $\hat{\mathcal{R}}^{Kth} = \sum_{l=0}^K C\hat{\mathcal{R}}_{(l)} \oplus CZ_K$. Then for any $\omega > 0$ there exists a $\Delta$ and $K$ such that

$dist[\hat{\mathcal{R}}^{Kth}, Reach^o(\mathcal{S}, X_0, t_0, [t_0, t_f])] < \omega$.

*Proof:* First consider the error caused by perturbation. Suppose $sup_{x_0 \in X_0} \|x_0\| < E$ for some $E > 0$. Then from Proposition 2, $\|Cz_K\| < \epsilon^{K+1} G_\infty(A_D, A_C, I)^K G_\infty(A, A_C, C)E$. Choose $K$ such that $\|Cz_K\| < \omega/3$. This implies

$$\begin{aligned}
dist(&Reach^o(\mathcal{S}, X_0, t_0, [t_0, t_f]), \\
&Reach^o(\bar{\mathcal{S}}, \bar{X}_0, t_0, [t_0, t_f])) < \omega/3
\end{aligned}$$

For the chosen expansion $K$, apply Corollary 1 using $\omega' = \frac{\omega}{3MK\|C\|}$ for all expansion $l \leq K$, this implies

$$\begin{aligned}
dist[C\hat{\mathcal{R}}_{(l)i}, Reach_{(l)i}(\bar{\mathcal{S}}, \bar{X}_0, t_0, [t_0, t_f])] < \frac{\omega}{3MK}, \\
\forall 0 \leq l \leq K, 1 \leq i \leq M
\end{aligned}$$

The proposition follows from the sum of the above two inequalities:

$$\begin{aligned}
& dist[\sum_{l=0}^K \sum_{i=1}^M C\hat{\mathcal{R}}_{(l)i} \oplus Cz_K, Reach^o(\mathcal{S}, X_0, t_0, [t_0, t_f])] \\
\leq & dist[\sum_{l=0}^K \sum_{i=1}^M C\hat{\mathcal{R}}_{(l)i}, Reach^o(\mathcal{S}, X_0, t_0, [t_0, t_f])] + \|Cz_k\| \\
< & MK \frac{\omega}{3MK} + dist[Reach^o(\mathcal{S}, X_0, t_0, [t_0, t_f]), \\
& Reach^o(\bar{\mathcal{S}}, \bar{X}_0, t_0, [t_0, t_f])] + \|Cz_K\| < \omega
\end{aligned}$$

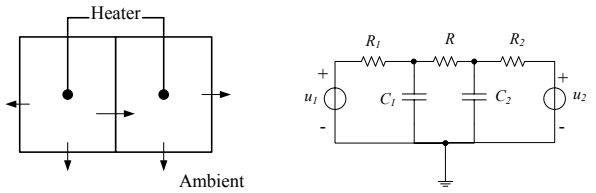
∎

## VI. Case Study

This section describes the application of the decomposition-based reachability analysis approach to two case studies: a two-room temperature system and a multi-machine electric power system. The reachability analysis procedure is implemented in MATLAB. All the computations are performed on a Pentium 4 PC with 1G RAM running Windows XP and MATLAB 7.0.1.

### A. Two-Room Temperature System

Consider two rooms heated by two heaters modeled as constant inputs. Figure 2(a) shows the conceptual model of the system, where heat transfer between rooms and the ambient environment is designated by arrows. The R-C circuit equivalent of the two-room temperature dynamics is shown in Fig. 2(b) where the temperatures of the rooms are equivalent to the voltages of the capacitors. The parameters for reachability analysis are $R_1 = 1$, $R_2 = 2$, $C_1 = 1$, $C_2 = 3$, $R_{12} = 100$ and $u_1 = u_2 = 1$.




(a) Temperature control systems (b) Equivalent R-C circuit model

Fig. 2. Dynamics of a two-room temperature control system.

Figure 3 shows the reach sets computed for the two-room temperature control system using the zeroth-order approximation and the first-order approximation. The state variables of the system are $\begin{bmatrix} u_{C_1} & u_{C_2} \end{bmatrix}^T$ The error bound estimate is $0.013$ for the zeroth-order approximation and $0.000256$ for the first-order approximation. Both the zeroth-order and the first-order approximation results give good over-approximations of the reach sets of the full-order system. The first-order approximation is almost indistinguishable from the result using the full-order model.

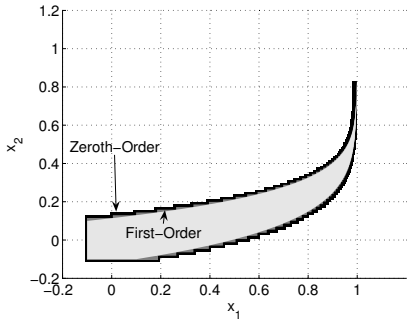



Fig. 3. The reach sets of the two-room temperature control system.

### B. Multi-Machine Power System

Consider the problem of computing reach sets for the load-frequency dynamics of the three-bus electric power system shown in Fig. 4. Two generators, both equipped with turbine governors, are connected to two buses, and each bus has a constant load. Both buses are connected to the environment modeled by an infinite bus.

Consider the case where the loads increase instantaneously at both buses and suppose we are interested in analyzing the response of the generator at bus 1. The transient of

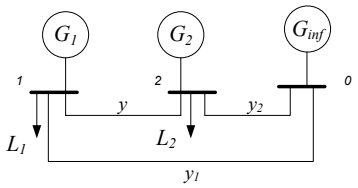



Fig. 4. A three-bus power system.

frequency is approximately modeled by an affine dynamic system $\mathcal{S}(A, b, C)$:

$$A = \begin{bmatrix} 0.0 & 1.0 & 0.0 & 0.0 & 0.0 & 0.0 \\ -4.02 & -2.0 & 2.0 & 0.02 & 0.0 & 0.0 \\ 0.0 & 1.0 & -2.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.0 & 1.0 & 0.0 \\ 0.02 & 0.0 & 0.0 & -2.02 & -2.0 & 2.0 \\ 0.0 & 0.0 & 0.0 & 0.0 & 1.0 & -2.0 \end{bmatrix}, b = \begin{bmatrix} 0 \\ -2 \\ 0 \\ 0 \\ -2 \\ 0 \end{bmatrix},$$

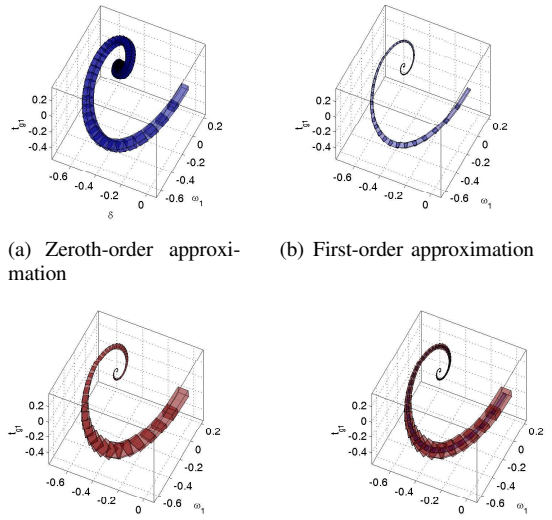
$C = \begin{bmatrix} I_3 & 0_{3\times 3} \end{bmatrix}$

The state variables of the electric power system are $x = \begin{bmatrix} \delta_1 & \omega_1 & t_{g1} & \delta_2 & \omega_2 & t_{g2} \end{bmatrix}^T$ [19]. The reach set is computed for the system. The results computed using zeroth-order, first-order approximations and using the full-order model are shown in Fig. 5. The computation time for the three reach sets are $0.851$, $2.053$ and $10.304$ seconds, respectively. The error bounds $\omega_K$ are estimated as $0.014817$ for the zeroth-order approximation and $0.000583$ for the first-order approximation.

It can be observed that although the full-order computation consumes as much as $5$ times the computation time as that using the first-order approximation, the reachability analysis using the full-order model does not even give a closer approximation than the first-order approximates for this example. This is because the convex hull (CH) cannot be used for the reach set in the full-order state space. The use of oriented rectangular hull (ORH), which is computed using more robust and efficient routines [16], introduces additional over-approximation errors to the computation. The zeroth-order approximation, which consumes only one tenth of the computation time, gives a reasonable approximation compared to the reach set computed using the full-order model. As shown in Fig. 5(d), the first-order approximation using the $\epsilon$-decomposition method is contained in the reach set computed using the full-order model, which means the approximation error caused by the $\epsilon$-decomposition is smaller than the error introduced in the ORH-based reach set computation.

## VII. Discussion

This paper presents an approach for reachability analysis for affine dynamic systems using $\epsilon$-decomposition techniques. The reach sets are computed using decomposed subsystem models rather than using the full-order model. An iterative method for reducing the approximation error is presented. It is shown that the reach set computed using the iterative computation can be made arbitrarily close to the reach set of the full-order system. The approach is illustrated by analyzing a temperature control system and an electric power network. Extension of the method to verify hybrid dynamic systems is currently under investigation.



(a) Zeroth-order approximation

(b) First-order approximation

(c) Using full-order model

(d) Comparison of results of first-order approximation and using full model

Fig. 5. Reach set computed using different order approximations.

## ACKNOWLEDGEMENT

This research was supported in part by the US Defense Advance Projects Research Agency (DARPA) contract nos. F33615-00-C-1701 and F33615-02-C-4029, US Army Research Office (ARO) contract no. DAAD19-01- 1-0485, and the US National Science Foundation (NSF) contract no. CCR-0121547.

## REFERENCES

[1] C. J. Tomlin, I. Mitchell, A. M. ayen, and M. Oishi, "Computational techniques for the verification of hybrid systems," *Proceedings of the IEEE*, vol. 91, no. 7, pp. 986– 1001, Jul 2003.

[2] R. Alur, T. A. Henzinger, and P.-H. Ho, "Automatic symbolic verification of embedded systems," *IEEE Trans. on Software Engineering*, vol. 22, no. 3, pp. 181–201, March 1996.

[3] I. Silva, O. Stursberg, B. H. Krogh, and S. Engell, "An assessment of the current status of algorithmic approaches to the verification of hybrid systems," in *Proc. 40th IEEE Conf. on Decision and Control*, Dec 2001, pp. 2867–2874.

[4] E. Asarin and T. Dang, "Abstraction by projection and application to multi-affine systems," in *Proceedings of Hybrid Systems: Computation and Control (HSCC'04)*. Springer-Verlag, 2004.

[5] Z. Han and B. H. Krogh, "Reachability analysis of hybrid systems using reduced-order models," in *IEEE Proc of American Control Conference (ACC'04)*, 2004.

[6] D. Stipanovic, I. Hwang, and C. Tomlin, "Computation of an over-approximation of the backward reachable set using subsystem level set functions," *Dynamics of Continuous, Discrete, and Impulsive Systems, Series A: Mathematical Analysis*, vol. 11, pp. 399–411, 2004.

[7] G. Frehse, Z. Han, and B. Krogh, "Assume-guarantee reasoning for hybrid i/o-automata by over-approximation of continuous interaction," in *IEEE Conference on Dicision and Control (CDC'2004)*, 2004.

[8] M. E. Szer and D. D. Siljak, "Nested epsilon-decompositions of linear systems, weakly coupled and overlapping blocks," in *Proceedings of the 1990 Bilkent Conference on New Trends in Communication, Control and Signal Processing*, vol. 1, 1990, pp. 827–842.

[9] D. D. Siljak, *Large-scale dynamic systems: stability and structure*, ser. North-Holland series in system science and engineering. Elsevier North-Holland Inc., 1978.

[10] P. V. Kokotovic, "Feedback design of large linear systems," in *Feedback Systems*, J. B. C. Jr., Ed. McGraw-Hill Book Company, 1972, pp. 99–137.

[11] J. R. E. O'Malley, *Singular perturbation methods for Ordinary Differential Equations*. Springer Verlag, 1991.

[12] V. Chellaboina, W. M. Haddad, D. S. Bernstein, and D. A. Wilson, "Induced convolution operator norms of linear dynamical systems," *Mathematics of Control, Signals, and Systems (MCSS)*, vol. 13, no. 3, pp. 216 – 239, September 2000.

[13] A. Chutinan and B. H. Krogh, "Compuational techniques for hybrid system verification," *IEEE Transaction on Automatic Control*, vol. 48, no. 1, pp. 64–75, Jan 2003.

[14] G. M. Ziegler, *Lectures on Polytopes*, ser. Graduate Texts In Mathematics. Springer-Verlag, 1995.

[15] N. S. Nedialkov, K. R. Jackson, and G. F. Corliss, "Validated solutions of initial value problems for ordinary differential equations," *Applied Mathematics and Computation*, vol. 105, pp. 21–68, 1999.

[16] O. Stursberg and B. H. Krogh, "On efficient representation and computation of reachable sets for hybrid systems," in *Hybrid Systems: Computation and Control HSCC'03*, ser. Springer-Series: LNCS 2623, 2003, pp. 482–497.

[17] T. Dang and O. Maler, "Reachability analysis via face lifting." in *HSCC*, 1998, pp. 96–109.

[18] P. Varaiya, "Reach set computation using optimal control," http://paleale.eecs.berkeley.edu/∼varaiya/papers_ps.dir/reachset.ps, 1998.

[19] M. D. Ilic and X. Liu, "A simple structural approach to modeling and analysis of the interarea dynamics of the large electric power systems," in *Proceedings of the North American Power Symposium*, 1993, pp. 560 – 578.