Proceeding of the 2004 American Control Conference
Boston, Massachusetts June 30 - July 2, 2004

Verifying Asymptotic Bounds for Discrete-Time Sliding Mode Systems with Disturbance Inputs

James Kapinski and Bruce H. Krogh
Department of Electrical and Computer Engineering
Carnegie Mellon University
{jpk3|krogh}@andrew.cmu.edu

***Abstract*— This paper presents a procedure for verifying asymptotic bounds on the behaviors of a class of discrete-time hybrid systems with disturbance inputs. First, an invariant set satisfying the given asymptotic bounds is computed. Then, conservative approximations of the reachable sets starting from the set of initial states are computed until the target invariant set is reached. Both steps in the procedure use LMI-based algorithms for computing minimal-volume ellipsoidal approximations to the actual reachable sets. The methods are particularly useful for analyzing the asymptotic behaviors of discrete-time sliding mode systems. The approach is illustrated for two examples.**

I. Introduction

This paper presents an approach to verifying properties of discrete-time sliding-mode systems (DTSMSs) using LMI-based methods for computing reachable sets and invariants for hybrid dynamic systems. The objective is to demonstrate that all trajectories of a DTSMS eventually satisfy specified bounds for given sets of initial states and disturbance inputs.

Sliding-mode controllers are usually designed as continuous-time sliding-mode systems (CTSMSs), but they are implemented using computers, which are inherently discrete-time [1], [2]. The problem with this approach is that it is not easy to guarantee properties of a DTSMS that results from the sample-data implementation of a CTSMS. Indeed, sampled-data implementations of CTSMSs can even be unstable [3], [4]. Consequently, the performance of the discrete-time implementation of a CTSMS is typically evaluated using simulation. Simulation studies cannot, however, verify the performance of the system for all possible disturbance inputs and a continuous range of initial states.

Many papers deal with various aspects of DTSMSs [5], [6]. We present a review of a representative subset of the literature on the subject. Koshkouei and Zinober discuss design of a DTSMS with disturbance inputs where the system reaches and remains on the sliding surface [7]. Their work, however, considers only known disturbances. Methods exist for designing DTSMSs that possess invariant regions, which the system is guaranteed to enter [8], [9], but these techniques do not apply to systems with disturbances. Tang and Misawa present a method to construct a discrete-time sliding mode controller that guarantees bounds on an invariant the boundary layer [10]. The size of the boundary layer depends on the constraints on the disturbance inputs. This latter work is most closely related to the problem considered in this paper, with the difference being that we are interested in verifying asymptotic convergence to a computed invariant set for a given DTSMS, rather than synthesizing a controller to achieve a particular bounded behavior.

In quasi-sliding-mode systems the state is guaranteed to continually cross the switching surface but is not constrained to reach and remain on the switching surface [6]. Our work addresses quasi-sliding-mode systems, strictly sliding-mode systems, and systems that do not satisfy the conditions for either of these classes of DTSMSs, such as systems that are discrete-time implementations of continuous-time sliding mode designs.

Systems with sliding modes can be modelled as hybrid systems. Here we consider the application of techniques for computing reachable sets for hybrid systems to the problem of verification of DTSMSs. Branicky shows that in some cases Lyapunov techniques can be used to show that switched systems are stable [11]. Hybrid system verification techniques can be used to show that switching systems satisfy safety properties [12], [13], [14], [15], but these techniques do not perform well for systems that exhibit Zeno-like behavior, such as sliding mode systems. Nevertheless, the reachable sets can be computed to find bounds on the behavior over a finite time horizon. For example, Villa et. al used the tool HyTech to verify a finite-time-horizon specification for a sliding mode control system for an automotive engine system [16].

In this paper, we propose a method to compute bounds on the asymptotic behavior of LTI DTSMSs with disturbance inputs by combining the computation of an invariant for the system with an efficient method for computing a conservative approximation of the transient system behavior. Ellipsoidal representations of the reachable sets and LMI computations [17] are used in both parts of the procedure. Our approach extends the methods developed by Kurzhanski and Vályi [18] for computing reachable sets using ellipsoids.

II. Problem Formulation

The following class of systems includes DTSMSs.

Definition 2.1: A discrete-time switched-mode system (DSS) is a tuple $\mathcal{S} = (I, \mathcal{X}, \mathcal{V}, \mathcal{D}, X_0)$, where:

- I is the finite set of *modes*;
- $\mathcal{X} = \{X_i\}_{i \in I}$ is a partition of the state space $\mathbb{R}^n$ (i.e., $\bigcup_{i \in I} X_i = \mathbb{R}^n$ and $X_i \bigcap X_j = \emptyset$ for $i \neq j$);

0-7803-8335-4/04/$17.00 ©2004 AACC

- $\mathcal{V} = \{V_j\}_{i\in I}$, is the collection of input disturbance sets for each mode, where for each $i \in I$, $V_i = \bigcup_{i\in\{1,\ldots,J_i\}} V_i^j$, with $V_i^j \subseteq \mathbb{R}^m$ for $j = 1,\ldots,J_i$;
- $\mathcal{D} = \{f_i\}_{i\in I}$ is the set of dynamics associated with each mode, where $f_i : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$; and
- $X_0 \subseteq \mathbb{R}^n$ is the set of initial conditions.

In this paper, we assume the continuous dynamics of the DSSs are linear; that is, for each $i \in I$, there are matrices A_i, B_i such that $f_i(x, v) = A_i x + B_i v$.

Definition 2.2: A sequence of states $(x_0, x_1, \ldots)$ is a *run* of a DSS $\mathcal{S}$ if $x_0 \in X_0$ and for all $k \geq 0$, if $x_k \in X_i$, then $x_{k+1} = f_i(x_k, v_k)$ for some $v_k \in V_i$. $\mathcal{R}_\mathcal{S}$ denotes the set of all runs of $\mathcal{S}$.

Given a DSS $\mathcal{S}$, $Reach(k)$ denotes the set of states reached at time k along some run of $\mathcal{S}$; that is,

$$Reach(k) = \{x | x = x_k \text{ for some } (x_0, x_1, \ldots) \in \mathcal{R}_\mathcal{S}\}.$$

We are interested in verifying that all runs for a given DSS eventually satisfy given bounds specified by a *target set* $F \subset \mathbb{R}^n$. The following definition characterizes this objective.

Definition 2.3: Given a DSS $\mathcal{S}$ and a set of states $F \subset \mathbb{R}^n$, $\mathcal{S}$ us said to be *uniformly asymptotically F-bounded* if there exists some k' such that for all $k \geq k'$, $Reach(k) \subseteq F$.

Remark 2.1: We note that a weaker form of asymptotic boundedness (that is not "uniform") would simply require that all runs eventually enter and remain in F. Our computational procedure will terminate, however, only when all runs enter the target set within some time k'. Therefore, we consider the problem of verifying uniform asymptotic boundedness.

We address the following problem in this work.

Problem 2.1: Given a DSS $\mathcal{S}$ and a region $F \subset \mathbb{R}^n$, determine if $\mathcal{S}$ is uniformly asymptotically F-bounded.

In applications, the set F represents bounds the system must eventually satisfy after some transient period, even when there are disturbance inputs. For DTSMSs, F will typically be some a boundary layer around the switching surface containing the equilibrium of the system without disturbance inputs. In the remainder of the paper, we assume a particular DSS $\mathcal{S}$ and a target set F are given. If $\mathcal{S}$ is uniformly asymptotically F-bounded, we call it *a-safe*.

We use the following notation in our procedure to compute the reachable states. For $X' \subseteq \mathbb{R}^n$, $V' \subseteq \mathbb{R}^m$, and $i \in I$,

$$Post_i(X', V') \triangleq \{x | x = f_i(x', v') \text{ for some } x' \in X' \text{ and } v' \in V'\}.$$

Note that the $Post_i$ operator applies the dynamics for mode i to all states in X' and inputs in V', even if these sets include states and inputs that are not defined for mode i. This freedom will be used to compute over approximations to the reachable sets for the DSS.

To verify that a system is a-safe, we use the concept of an invariant set.

Definition 2.4: [19] A set of states $W \subseteq \mathbb{R}^n$ is a (positively) *invariant set* if

$$\bigcup_{i\in I} \bigcup_{j\in 1,\ldots,J_i} Post_i(W \cap X_i, V_i^j) \subseteq W.$$

An ellipsoid $\mathcal{E}(x_c, Q) \subset \mathbb{R}^n$ is defined as

$$\mathcal{E}(x_c, Q) = \{x : l^T x \leq l^T x_c + \sqrt{l^T Q l},\ \forall l \in \mathbb{R}^n\},$$

where $x_c \in \mathbb{R}^n$ and $Q \in \mathbb{R}^n \times \mathbb{R}^n$ is a symmetric, positive semidefinite matrix.

The support function of a set $X \subseteq \mathbb{R}^n$ is defined as

$$\rho(l|X) = \sup_{x\in X} l^T x,$$

where $l \in \mathbb{R}^n$. The support function identifies a supporting hyperplane of the set X for each direction vector l. The the set of points $x \in \mathbb{R}^n$ for which $l^T x = \rho(l|X)$ is a supporting hyperplane of X. Note that

$$\rho(l|\mathcal{E}(x_c, Q)) = l^T x_c + \sqrt{l^T Q l}.$$

III. Verifying a DSS is A-Safe

In this section we propose a procedure for proving that an DSS is a-safe. The technique we propose consists of first computing an invariant set for the system and then performing reachset computations. If the conservatively estimated reachset at any time increment is contained within the invariant set, the system is a-safe and the estimate of the computed reachset contains all of the behaviors of the system for all time.

A. Computing an Invariant

The following proposition allows us to construct an invariant ellipsoid for DSS's.

Proposition 3.1: Consider a DSS with ellipsoidal input sets, $V_i^j = \mathcal{E}(v_i^j, Q_i^j) \subseteq \mathcal{R}^m$. If there exists a P such that $A_i^T P A_i - P < 0$ for all i, then for all $x_c \in \mathbb{R}^n$, $Inv = \mathcal{E}(x_c, \alpha^*(x_c)Q)$ is an invariant for system $\mathcal{S}$, where

$$\alpha^*(x_c) = \max\{\alpha(x_c, i, V_i^j) | i \in \{1,\ldots,I\}, j \in \{1,\ldots,J_i\}\} \quad (1)$$

$$\alpha(x_c, i, V_i^j) = \frac{(\|A_i x_c + B_i v_i^j - x_c\| + \lambda^{max}_{B_i Q_i^j B_i^T})^2}{\epsilon_i^2} \quad (2)$$

$$\epsilon_i = \min_{l^T l = 1} \sqrt{l^T Q l} - \sqrt{l^T A_i Q A_i^T l}, \quad (3)$$

where $Q = P^{-1}$, and $\lambda^{max}_{B_i Q_i^j B_i^T}$ is the maximum eigenvalue of $B_i Q_i^j B_i^T$.

The proof of Prop. 3.1 uses the following lemma.

Lemma 3.1: For a DSS $\mathcal{S}$, if Q is a solution to $A_i^T P A_i - P < 0$, where $P = Q^{-1}$, $\hat{\alpha} > \alpha$, and $Post_i(\mathcal{E}(x_c, \alpha Q), V_i^j) \subseteq \mathcal{E}(x_c, \alpha Q)$, then $Post_i(\mathcal{E}(x_c, \hat{\alpha} Q), V_i^j) \subseteq \mathcal{E}(x_c, \hat{\alpha} Q)$.

Proof: We prove by contradiction. Let $Post_i(\mathcal{E}(x_c, \alpha Q), V_i^j) \subseteq \mathcal{E}(x_c, \alpha Q)$, $\hat{\alpha} > \alpha$, and assume

$Post_i(\mathcal{E}(x_c, \hat{\alpha}Q), V_i^j) \nsubseteq \mathcal{E}(x_c, \hat{\alpha}Q)$. Then there exists an l such that $\rho(l|Post_i(\mathcal{E}(x_c, \hat{\alpha}Q), V_i^j)) - \rho(l|\mathcal{E}(x_c, \hat{\alpha}Q)) > 0$. For this l,

$$l^T(A_i x_c + B_i v_i^j - x_c) + \sqrt{\hat{\alpha}}\sqrt{l^T A_i Q A_i^T l} + \sqrt{l^T B_i Q_u B_i^T l} - \sqrt{\hat{\alpha}}\sqrt{l^T Q l} > 0. \quad (4)$$

Since $Post_i(\mathcal{E}(x_c, \alpha Q), V_i^j) \subseteq \mathcal{E}(x_c, \alpha Q)$,

$$\begin{aligned} \rho(l|Post_i(\mathcal{E}(x_c, \alpha Q), V_i^j)) - \rho(l|\mathcal{E}(x_c, \alpha Q)) \leq 0 \\ l^T(A_i x_c + B_i v_i^j - x_c) + \sqrt{\alpha}\sqrt{l^T A_i Q A_i^T l} + \\ \sqrt{l^T B_i Q_u B_i^T l} - \sqrt{\alpha}\sqrt{l^T Q l} \leq 0. \end{aligned} \quad (5)$$

Multiplying (5) by -1 and adding it to (4),

$$\begin{aligned} (\sqrt{\hat{\alpha}} - \sqrt{\alpha})\sqrt{l^T A_i Q A_i^T l} - \\ (\sqrt{\hat{\alpha}} - \sqrt{\alpha})\sqrt{l^T Q l} &> 0, \\ (\sqrt{\hat{\alpha}} - \sqrt{\alpha})(\sqrt{l^T A_i Q A_i^T l} - \sqrt{l^T Q l}) &> 0, \\ (\sqrt{\hat{\alpha}} - \sqrt{\alpha})(\rho(l|\mathcal{E}(0, A_i Q A_i^T)) - \\ \rho(l|\mathcal{E}(0, Q)) &> 0. \end{aligned} \quad (6)$$

Because $\hat{\alpha} > \alpha$,

$$(\sqrt{\hat{\alpha}} - \sqrt{\alpha}) > 0. \quad (7)$$

It can be shown that since Q is a solution to $A_i^T P A_i - P < 0$, where $P = Q^{-1}$, then $\mathcal{E}(0, A_i Q A_i^T) \subseteq \mathcal{E}(0, Q)$, which implies

$$\rho(l|\mathcal{E}(0, A_i Q A_i^T)) - \rho(l|\mathcal{E}(0, Q)) \leq 0. \quad (8)$$

Relations (7) and (8) contradict (6), and so the assumption is invalid.

■

Proof of Prop. 3.1: Let $\hat{Q} = A_i Q A_i^T$ and $\alpha = \alpha(x_c, i, V_i^j)$. $\mathcal{E}(0, \alpha\hat{Q}) \subseteq \mathcal{E}(0, \alpha Q)$ since αQ satisfies the Lyapunov equation $A_i^T P A_i - P < 0$. The minimum distance of a point in $\mathcal{E}(0, \alpha\hat{Q})$ to a point on the perimeter of $\mathcal{E}(0, \alpha Q)$ is given by

$$\begin{aligned} \hat{\epsilon}_i &= \min_{l^T l = 1} \rho(l|\mathcal{E}(0, \alpha Q)) - \rho(l|\mathcal{E}(0, \alpha\hat{Q})) \\ &= \min_{l^T l = 1} \sqrt{\alpha}\sqrt{l^T Q l} - \sqrt{\alpha}\sqrt{l^T \hat{Q} l}. \end{aligned} \quad (9)$$

It can be shown that $\hat{\epsilon}_i$ is given by

$$\hat{\epsilon}_i = \|A_i x_c + B_i v_i^j - x_c\| + \lambda^{max}_{B_i Q_i^j B_i^T},$$

which is nonnegative since $B_i Q_i^j B_i^T$ is positive semidefinite. Now consider

$$\begin{aligned} \tilde{\epsilon}_i &= \min_{l^T l = 1} \rho(l|\mathcal{E}(x_c, \alpha Q)) - \rho(l|Post_i(\mathcal{E}(x_c, \alpha Q), V_i^j)) \\ &= \min_{l^T l = 1} \rho(l|\mathcal{E}(x_c, \alpha Q)) - \rho(l|\mathcal{E}(A_i x_c, \alpha\hat{Q})) - \\ &\qquad \rho(l|\mathcal{E}(B_i v_i^j, B_i Q_i^j B_i^T)) \qquad (10) \\ &= \min_{l^T l = 1} l^T(x_c - A_i x_c - B_i v_i^j) + \sqrt{\alpha}\sqrt{l^T Q l} - \\ &\qquad \sqrt{\alpha}\sqrt{l^T \hat{Q} l} - \sqrt{l^T B_i Q_i^j B_i l}. \qquad (11) \end{aligned}$$

If $\tilde{\epsilon}_i \geq 0$, then $Post(\mathcal{E}(x_c, \alpha Q), V_i^j)) \subseteq \mathcal{E}(x_c, \alpha Q)$. A lower bound on $\sqrt{\alpha}\sqrt{l^T Q l} - \sqrt{\alpha}\sqrt{l^T \hat{Q} l}$ is given by $\hat{\epsilon}_i$. It can be shown that a lower bound on the remaining two terms is given by $-\hat{\epsilon}_i$, which leads to $\tilde{\epsilon}_i \geq 0$. Since $\alpha^*(x_c) \geq \alpha(x_c, i, V_i^j)$ for all i and V_i^j, by Lemma 3.1, $Post(\mathcal{E}(x_c, \alpha^*(x_c)Q), V_i^j)) \subseteq \mathcal{E}(x_c, \alpha^*(x_c)Q)$ for all i and V_i^j, which means that $\mathcal{E}(x_c, \alpha^*(x_c)Q)$ is an invariant of system $\mathcal{S}$.

■

Remark 3.1: LMI techniques can be used to compute a P that satisfies the simultaneous Lyapunov stability equations $A_i^T P A_i - P < 0$ [17]. Also, optimization (3) is a convex, nonlinear program. Therefore, the invariant Inv, defined in Prop. 3.1 can be found numerically for a given DSS.

To verify that a DSS $\mathcal{S}$ is a-safe using our procedure, two conditions must be satisfied: an invariant set of $\mathcal{S}$, Inv, must be found that is contained in F, and the reachset estimate at some time increment must be contained in Inv. To make it easier to satisfy the latter condition, Inv should be as large as possible while still being contained in F.

If the invariant provided by Prop. 3.1 is not contained within F, the shrinking procedure shown in Fig. 1 is performed to reduce the size of Inv. The shrinking procedure requires a description of an DSS $\mathcal{S}$ and an invariant set for $\mathcal{S}$, Inv. Two operations are also required to perform the shrinking procedure: $\hat{Post}$, which is defined in Sect. III-B, and $Wrap$. $Wrap(\hat{Post}, Inv)$ is the minimum volume ellipsoid such that $\hat{Post} \subseteq Wrap(\hat{Post}, Inv) \subseteq Inv$, which can be computed by solving an LMI. If such an ellipsoid does not exist, $Wrap(\hat{Post}, Inv) = Inv$. Successive iterations of the outer loop are guaranteed to produce invariant ellipsoids of monotonically decreasing volume. If the shrinking procedure halts, a new invariant set Inv is produced such that $Inv \subseteq F$.

If the invariant set Inv provided by Prop. 3.1 is strictly contained in F, the size of Inv can be increased by multiplying the configuration matrix by a number $\gamma > 1$. By Lemma 3.1, if $\mathcal{E}(x_c, Q)$ is an invariant for LSMS $\mathcal{S}$, then $\mathcal{E}(x_c, \gamma Q)$ is also an invariant for $\mathcal{S}$. If F is given by a set of linear constraints, then the maximum value that γ can take is given by

$$\gamma = \min\left\{\frac{(d_1 - C_1 x_c)^2}{C_1 Q C_1^T}, \ldots, \frac{(d_W - C_W x_c)^2}{C_W Q C_W^T}\right\},$$

/* Invariant Inv of DSS system $\mathcal{S}$ is known */
While $Inv \nsubseteq F$
  $\hat{Post} := \emptyset$
  For each $i \in \{i, \ldots, I\}$
    For each $V_i^j \in \hat{V}_i$
      $\hat{Post} := \hat{Post} \cup \hat{Post}_i(Inv, V_i^j)$
  Compute $\mathcal{E}^* := Wrap(\hat{Post}, Inv)$
  /* $\mathcal{E}^*$ is a new invariant of DSS system $\mathcal{S}$ */
  $Inv := \mathcal{E}^*$

Fig. 1. Invariant shrinking procedure: reduces the size of the invariant given by Prop. 3.1.

where $Inv = \mathcal{E}(x_c, Q)$, and for each $w \in \{1, \ldots, W\}$, $C_w \in \mathbb{R}^{1\times n}$ and $d_w \in \mathbb{R}$, with $R = \{x | C_w x \leq d_w, \forall w \in \{1, \ldots, W\}\}$.

B. Reachset Computations

The procedure for determining if a DSS system $\mathcal{S}$ is a-safe is shown in Fig. 2. The procedure uses an efficient method for estimating the set of reachable states, which involves merging sets of points together that are close to each other, in some sense. This technique is related to the systematic simulation scheme described in [20].

At the beginning of the k^{th} iteration of the outer loop of the DSS verification procedure, the union of the sets in $queue_{new}$ contains a conservative estimate of $Reach(k)$. If, at the beginning of the k^{th} iteration, $queue_{new}$ is empty, the estimate of $Reach(k-1)$ is contained in Inv. In this case, the system is a-safe, and the procedure halts.

The verification procedure requires three functions: $\hat{Post}$, $Dist$, and $Merge$. The $\hat{Post}$ function is an estimate of $Post$, which is performed using ellipsoidal calculus techniques developed by Kurzhanski and Vályi [18]. If $\mathcal{E}_X = \mathcal{E}(x_c, Q_X) \subset \mathbb{R}^n$ and $\mathcal{E}_V = \mathcal{E}(v_c, Q_V) \subset \mathbb{R}^m$, $\hat{Post}_i(\mathcal{E}_X, \mathcal{E}_V)$ is given by

$$\hat{Post}_i(\mathcal{E}_X, \mathcal{E}_V) = \mathcal{E}(A_i x_c + B_i v_c, \tilde{Q}),$$

and

$$\tilde{Q} = (1 + \sqrt{\frac{tr(B_i Q_V B_i^T)}{tr(A_i Q_X A_i^T)}}) A_i Q_X A_i^T + (1 + \sqrt{\frac{tr(A_i Q_X A_i^T)}{tr(B_i Q_V B_i^T)}}) B_i Q_V B_i^T,$$

with $tr(Q)$ being the trace of Q. $\hat{Post}_i(\mathcal{E}_X, \mathcal{E}_V)$ is the ellipsoid with the minimum sum of squares of semiaxes that contains $Post(\mathcal{E}_X, \mathcal{E}_V)$.

The $Dist$ function is some metric on ellipsoidal sets. Intuitively, the metric should represent the distance between two sets. For our examples, we use $Dist(\mathcal{E}(x_c, Q), \mathcal{E}(x'_c, Q')) = \|x_c - x'_c\|_2$. The constant c must be selected as the merging criterion, such that if two ellipsoids $\mathcal{E}$ and $\mathcal{E}'$ satisfy $Dist(\mathcal{E}, \mathcal{E}') \leq c$, then sets $\mathcal{E}$ and $\mathcal{E}'$ will be merged into one region.

$Merge(\mathcal{E}, \mathcal{E}')$ computes the minimum volume ellipsoid that contains the ellipsoids $\mathcal{E}$ and $\mathcal{E}'$ using an LMI based optimization technique (see [17], page 43).

/* Invariant Inv of DSS system $\mathcal{S}$ is known */
$queue_{new} := Inv$
While $queue_{new} \neq \emptyset$
  $queue := queue_{new}$
  $queue_{new} := \emptyset$
  /* Estimate $Post_i(\mathcal{E}, V_i^j)$ for each element of $queue$ and each relevant i and V_i^j */
  For each $\mathcal{E} \in queue$
    For each $i \ni \mathcal{E} \cap X_i \neq \emptyset$
      For each $V_i^j \in \hat{V}_i$
        Compute $\hat{\mathcal{E}} := \hat{Post}_i(\mathcal{E}, V_i^j)$
        /* If $\hat{\mathcal{E}}$ is close to some element of $queue_{new}$, merge the two sets */
        If $\exists \tilde{\mathcal{E}} \in queue_{new} \ni Dist(\tilde{\mathcal{E}}, \hat{\mathcal{E}}) \leq c$
          Replace $\tilde{\mathcal{E}}$ in $queue_{new}$ with $Merge(\tilde{\mathcal{E}}, \hat{\mathcal{E}})$
        /* If $\hat{\mathcal{E}}$ is not contained within Inv, add $\hat{\mathcal{E}}$ to $queue_{new}$ */
        Elseif $\hat{\mathcal{E}} \nsubseteq Inv$
          Add $\hat{\mathcal{E}}$ to $queue_{new}$

Fig. 2. DSS verification procedure: used to show that the reachset of a DSS enters an invariant region.

IV. Examples

Consider the following example, DSS $\mathcal{S}_1$, from [3].

$$\begin{aligned} A_i &= \begin{bmatrix} 1 & .05 \\ -.056 - .055k_{1_i} & 1.2 - .055k_{2_i} \end{bmatrix} \\ B_i &= \begin{bmatrix} 0 \\ .05 \end{bmatrix} \\ k_{1_1} \cdots k_{1_4} &= 138 \\ k_{2_1} &= k_{2_3} = 36 \\ k_{2_2} &= k_{2_4} = 14 \\ X_0 &= \mathcal{E}([3\ 0]^T, I^{2\times 2}) \\ V_i &= \{v | 0 < v < 1\}, \end{aligned}$$

where $I^{2\times 2}$ is the two-by-two identity matrix. The partition elements, shown in Fig. 3, are defined by $x_2 = 0$ and the zeros of the switching function $s(x) = Cx$, where $C = [20\ 1]$. Fig. 3 shows a run of length 30, with $x_0 = (1, 1)$, for system $\mathcal{S}_1$.

The target set is given by $F = \{x | Cx \leq \sqrt{CC^T}, -Cx \leq \sqrt{CC^T}\}$. Our verification procedure was performed on $\mathcal{S}_1$ in order to show that $\mathcal{S}_1$ is uniformly asymptotically F-bounded.

The merging operation used in the verification procedure (Fig. 2) addresses the problem of searching several reachset paths. Fig. 4 illustrates this issue for the $\mathcal{S}_1$ system.

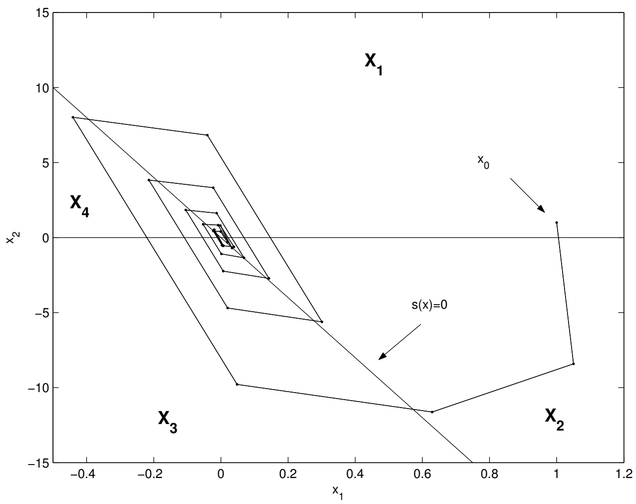

Fig. 3. DSS $\mathcal{S}_1$, with regions $X_1 \cdots X_4$, and a representative run of length 30 with a particular disturbance input.

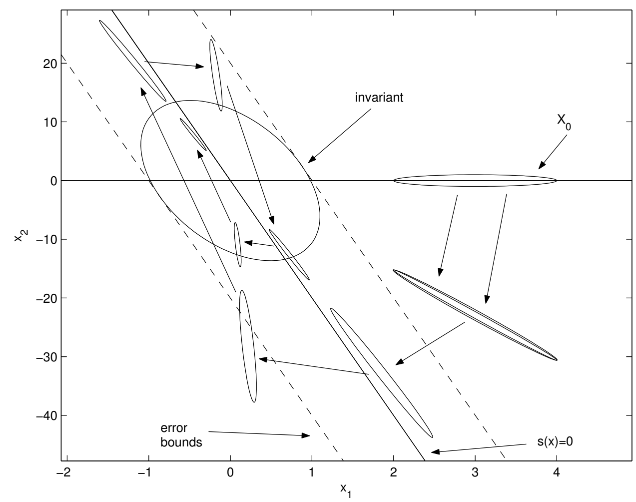

Fig. 5. Verification of system $\mathcal{S}_1$. Reachset estimation enters the invariant region, and so $\mathcal{S}_1$ is uniformly asymptotically F-bounded.

The Fig. shows the initial condition set X_0 and the first two estimations of the $Post$ operator. The $Post_1(X_0, V_i)$ and $Post_2(X_0, V_i)$ estimations are performed because X_0 intersects regions 1 and 2. The two ellipsoidal regions are merged together by computing an ellipsoid that contains them. In doing so, only one region must be propagated forward on the next iteration instead of two.

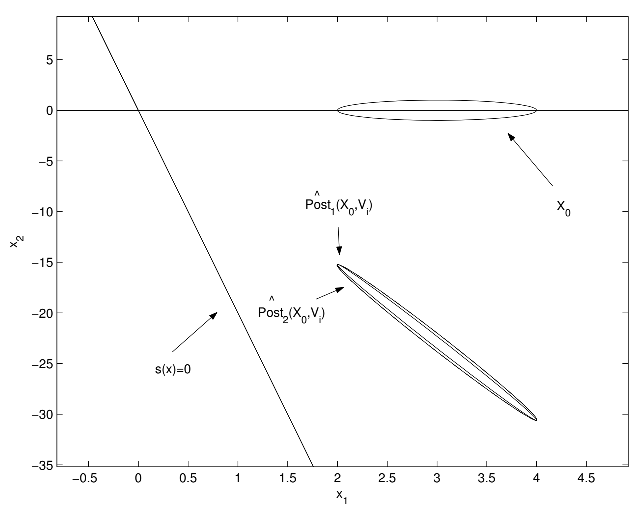

Fig. 4. First two reachset computations and first merging operation for system $\mathcal{S}_1$

An invariant for system $\mathcal{S}_1$ was found using Prop. 3.1. The invariant was scaled up so as to be supported by the error bounds for the system. The reachset computations then proceeded from X_0. After 8 iterations (.84 seconds)[1] the reachset was found to be contained within the invariant. The estimated reachset contains the behaviors of the system over an infinite time horizon. Fig. 5 illustrates the results.

[1]Computation times are given for a Pentium 4, 2.8 GHz processor machine with 512 MB of RAM, running Windows XP.

As a second example, we consider a linearization of the automotive engine air/fuel ratio (AFR) control system described in [21]. The system is a DSS, $\mathcal{S}_2$, with

$$A_1 = A_2 = \begin{bmatrix} 0.945 & 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.990 & 0.004 & 0.0 & 0.0 \\ 0.0 & -0.004 & 0.990 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.990 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.0 & 0.988 \end{bmatrix},$$

$$B_1 = B_2 = \begin{bmatrix} 0.0 \\ 0.027 \\ 0.012 \\ -0.027 \\ 0.0 \end{bmatrix},$$

$$V_1 = 1.0, V_2 = -1.0,$$

$$X_0 = \mathcal{E}(x_0, Q_0),$$

where

$$x_0 = \begin{bmatrix} 7.0 \\ 7.0 \\ 7.0 \\ 7.0 \\ 7.0 \end{bmatrix}, Q_0 = I^{5\times 5}.$$

$X_1 = \{x | C^T x \leq d\}$, and $X_2 = \{x | C^T x > d\}$, where $d = 0.044$ and

$$C = \begin{bmatrix} -3.070 \times 10^{-4} \\ 0.0 \\ 0.0 \\ -4.994 \times 10^{-2} \\ 1.300 \times 10^{-2} \end{bmatrix}.$$

In this case, the switching function, $s(x) = C^T x - d$, is the deviation of the AFR from it's nominal value of 14.681. The target region is given by $F = \{x| \; |s(x)| \leq 0.367\}$. This corresponds to a 2.5% deviation of the AFR from the nominal value. Our procedure was used to construct an invariant that is contained in F. Then, the reachset from X_0 was computed and was found to enter the invariant set. The procedure terminated in 36.89 seconds after the 114^{th} time increment. Fig. 6 shows several projections of the reachset estimates and the invariant ellipsoid.

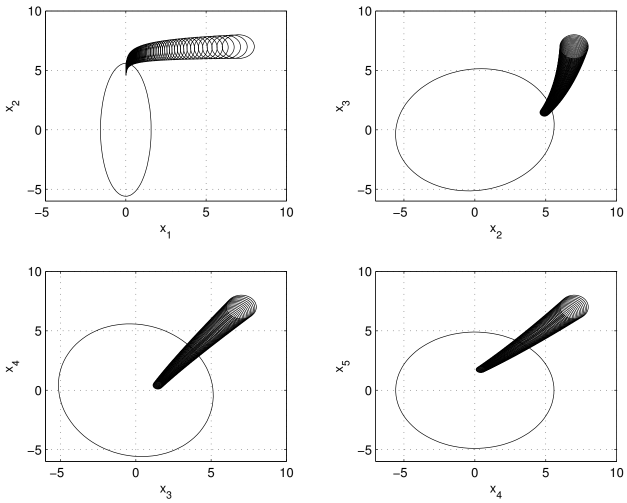

Fig. 6. Various projections of the verification of system $\mathcal{S}_2$

V. Conclusions

This paper presents a method for verifying asymptotic bounds on the behaviors of discrete-time sliding mode systems. The procedure is a based on a new method for computing invariant sets for linear switched mode systems with ellipsoidal inputs. New methods for making reachable set computations more efficient are also introduced. The invariant sets are used as the termination condition for the reachable set computations to characterize the behaviors of systems over an infinite time horizon.

The invariant construction presented in this work is not guaranteed to find a satisfactory invariant. The invariants produced using our procedure may be too large to be useful, and the invariant shrinking procedure presented in Sect. III-A may not terminate. One issue we are pursing is identifying proper halting conditions for the invariant shrinking procedure.

In order to successfully verify a system, the estimations of the reachset must enter an invariant region. This may not occur either because the system allows behaviors that never enter the invariant region or because the conservativeness of the reachset estimation introduces behaviors that are not realizable by the system and do not converge to the invariant set. To address the latter problem, an efficient method of refining the reachset computations, to make the reachset estimations less conservative, must be developed.

Currently, our merging conditions are based on heuristics. We are investigating intelligent methods of selecting merging conditions.

Acknowledgements

This research was supported in part by Ford, 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] J. Hung, W. Gao, and J. Hung, "Variable structure control: a survey," *IEEE Transactions on Industrial Electronics*, vol. 40, no. 1, pp. 2–22, February 1993.

[2] V. Utkin, "Variable structure systems with sliding modes," *IEEE Transactions on Automatic Control*, vol. AC-22, no. 2, pp. 212–222, April 1977.

[3] S. Sarpturk, Y. Istefanopulos, and O. Kaynak, "On the stability of discrete-time sliding mode control systems," *IEEE Transactions on Automatic Control*, vol. 32, no. 10, pp. 930–932, 1987.

[4] K. Furuta, "Sliding mode control of a discrete system," *Syst. Contr. Lett.*, vol. 14, pp. 145–152, 1990.

[5] X. Yu, *Variable Structure and Lyapunov Control*. Springer-Verlag, 1994, ch. 7, Digital variable structure control with psuedo-sliding modes, pp. 133–155.

[6] C. Milosavljević, "General conditions for the existence of a quasisliding mode on the switching hyperplane in discrete variable structure systems," *Automation and Remote Control*, vol. 46, no. 3, pp. 307–314, 1985.

[7] A. Koshkouei and A. Zinober, "Sliding mode control of discrete-time systems," *Journal of Dynamic Systems, Measurement and Control*, vol. 122, pp. 793–802, December 2000.

[8] W. Gao, Y. Wang, and A. Homaifa, "Discrete-time variable structure control systems," *IEEE Transactions on Industrial Electronics*, vol. 42, no. 2, pp. 117–122, April 1995.

[9] X. Yu and S. Yu, "Discrete sliding mode control design with invariant sliding sectors," *ASME Journal of Dynamic Systems, Measurement, and Control*, vol. 122, pp. 776–782, December 2000.

[10] C. Tang and E. Misawa, "Discrete variable structure control for linear multivariable systems," *Journal of Dynamic Systems, Measurement and Control*, vol. 122, pp. 783–791, December 2000.

[11] M. Branicky, "Multiple lyapunov functions and other analysis tools for switched and hybrid systems," vol. 43, no. 4, pp. 475–482, 1998.

[12] A. Chutinan and B. Krogh, "Verification of infinite state dynamic systems using approximate quotient transition systems," *IEEE Transactions on Automatic Control*, vol. 46, no. 9, pp. 1401–1410, Sept. 2001.

[13] S. Kowalewski, S. Engell, J. Preussig, and O. Stursberg, "Verification of logic controllers for continuous plants using timed condition/event-system models," *Automatica*, vol. 35, pp. 505–518, 1999.

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

[15] O. Botchkarev and S. Tripakis, "Verification of hybrid systems with linear differential inclusions using ellipsoidal approximations," in *Hybrid Systems: Computation and Control, 3rd International Workshop, HSCC'00*, N. Lynch and B. Krogh, Eds. Springer-Verlag, 2000.

[16] T. Villa, H. Wong-Toi, A. Balluchi, J. P. ig, A. Sangiovanni-Vincentelli, and Y. Watanabe, "Formal verification of an automotive engine controller in cutoff mode," in *37th IEEE Conference on Decision and Control*, December 1998, pp. 4271–4276.

[17] S. Boyd, L. Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*, ser. SIAM Studies in Applied Mathematics. SIAM, 1994, vol. 15.

[18] A. B. Kurzhanski and I. Vályi, *Ellipsoidal Calculus for Estimation and Control*. Boston: Birkhä user, 1997.

[19] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, pp. 1747–1767, 1999.

[20] J. Kapinski, O. Maler, O. Stursberg, and B. H. Krogh, "On systematic simulation of open continuous systems," in *Hybrid Systems: Computation and Control, 6th International Workshop, HSCC'03*. Springer-Verlag, 2003, pp. 283–297.

[21] T. Simsek, "Technical overview of the expanded powertrain challenge problem," 2002, http://vehicle.me.berkeley.edu/mobies/presentations/ExpandedPowerTrainChallengeProblem.pdf.