15th Triennial World Congress, Barcelona, Spain

ROBUST VERIFICATION OF PIECEWISE AFFINE SYSTEMS

Jacob Roll

Division of Automatic Control, Department of Electrical Engineering, Linköping University, SE-581 83 Linköping, Sweden. E-mail: roll@isy.liu.se

Abstract: Piecewise affine systems is an important class of hybrid systems. They consist of several affine dynamic subsystems, between which switchings occur at different occasions. In this paper, a verification method for piecewise affine systems is considered, and a method to determine how sensitive the verified properties are to changes in the dynamics and the locations of the switching surfaces is proposed. This information can then be used for robustness analysis or control design. *Copyright ©2002 IFAC*

Keywords: Verification, Robustness, Bounded disturbances, Uncertain dynamic systems, Switching surfaces

1. INTRODUCTION

Piecewise affine systems constitute a special class of hybrid systems. These systems consist of several affine subsystems, between which switchings occur at different occasions. In this paper, the piecewise affine systems will be on the form

$$\dot{x} = A(v)x + b(v), \quad x \in X(v) \tag{1}$$

where v is a piecewise constant function of x. This implies that the dynamics of a trajectory $x(t)$ just depends on x, not on t or on any external input. The different regions $X(v)$ are assumed to be polyhedra. Systems of this kind occur in many applications. A very simple example could be a linear system, controlled by linear feedback, but where the control signal is bounded.

Verification of hybrid systems is a research field that has received much attention in recent years. General verification and reachability problems may be very difficult, or even undecidable, except for some classes of systems (Alur *et al.*, 2000). Therefore, many approximating methods have been proposed (Bemporad *et al.*, 2000; Chutinan, 1999; Einarsson, 2000; Engell *et al.*, 2000). The problems considered in this paper arise for example when considering robustness aspects of one of the methods proposed by Einarsson (2000), which is a method for verification of piecewise affine switched systems. In this method, the behaviour of the vector field $\dot{x}(t)$ at the borders of the regions $X(v)$ is analysed. Specifically, questions such as "At a given face of the polyhedron $X(v)$, is there a point, x_0, such that $\dot{x}_0$ is pointing out of $X(v)$, or are all trajectories at this face going into $X(v)$?" are answered (this kind of computations has also been used, e.g., by Johansson (1999)). This is used to determine which transitions between different regions are possible, and if transitions are guaranteed to occur non-deterministically (i.e., one transition out of a set of transitions from a given polyhedron is guaranteed to occur). Then finite automata are constructed, showing the guaranteed or possible transitions. They give an approximation of the system, and can be used for different kinds of verification. For example, it can be guaranteed that certain states in the original system are not reachable from a set of initial states, by proving that there is no sequence of possible transitions in the finite automata, taking the system state from the region of the initial states to the region of the final states.

Like all other methods mentioned above, the method by Einarsson (2000) assumes that a model of the system is given. It would be desirable to be able to determine how sensitive the approximating automata are to changes in the underlying systems, both in the dynamics and in the switching surfaces. Such information could be used to get a measure of how robust the verification process is to model errors, or as an aid in a control design process, if the system dynamics is to be adjusted without losing the verified property.

Since the approximating method considers the behaviour of $\dot{x}(t)$ at the borders of the regions $X(v)$, it must be determined how this behaviour changes with varying $A(v)$ and $b(v)$, and with translations of the surfaces that bound $X(v)$. In (Roll, 2000), the case of varying $A(v)$ and $b(v)$ was studied. Here one further step is taken, by considering also the case when the boundaries of the regions of $X(v)$ are uncertain.

The paper is organised as follows: In Section 2, the problem is formulated, and necessary notation is introduced. In Section 3, the results from (Roll, 2000) are summarised. The results concerning translations of the boundaries of $X(v)$ are given in Section 4, and finally, an example is given.

2. NOTATION AND PROBLEM FORMULATION

The systems considered in this paper are on the form

$$\begin{aligned} \dot{x} &= (A(v)-\Delta(v))x+b(v)-\delta(v), \\ x &\in X(v), \;\; v\in\{-1,0,1\}^M \end{aligned} \tag{2}$$

where $A(v)\in\mathbb{R}^{n\times n}$, $b(v)\in\mathbb{R}^n$ are given for all v. The vector v is a *key vector*, which is connected to $X(v)$. The regions $X(v)\subset\mathbb{R}^n$ are *polyhedra*, i.e., they are regions defined by linear inequalities. The separating hyperplanes are defined by

$$\{x\in\mathbb{R}^n \mid C_i x = d_i+\gamma_i\}, \;\; i=1,\ldots,M \tag{3}$$

where $C_i\in\mathbb{R}^{1\times n}$ and $d_i\in\mathbb{R}$ are given. The role of $\Delta(v)$, $\delta(v)$, and γ_i will be treated below. To allow for a compact representation, let C_i form the rows in an $M\times n$ matrix C, and collect d_i and γ_i into the vectors d and γ, respectively.

Now v is defined according to the following rule:

$$v_i = \begin{cases} -1 & \text{if } C_i x < d_i+\gamma_i \\ 0 & \text{if } C_i x = d_i+\gamma_i \\ 1 & \text{if } C_i x > d_i+\gamma_i \end{cases} \tag{4}$$

In this way there is a one-to-one relationship between v and $X(v)$. Note that a nonempty $X(v)$ will be contained in an $(n-1)$-dimensional affine subspace of $\mathbb{R}^n$ if and only if there is at least one zero entry in v. Nonempty polyhedra $X(v)$ corresponding to vectors v with no zero entries will be called *full-dimensional* polyhedra.

The matrices $\Delta(v)\in\mathbb{R}^{n\times n}$, $\delta(v)\in\mathbb{R}^n$ and $\gamma\in\mathbb{R}^M$ can be viewed either as uncertainties in the model, or as matrices of our choice. Only values of γ that do not affect the topology of the state-space partition compared to the case $\gamma=0$ will be allowed, i.e., the regions $X(v)$ will always have the same number of faces and the same neighbours as they would have if the separating hyperplanes were defined by $C_i x = d_i$. Without this requirement, regions may disappear when changing γ, and new regions – for which the system dynamics is not known – can be created.

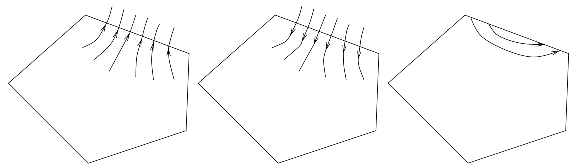

Fig. 1. Three options for the behaviour of the trajectories in the vicinity of a polyhedron face.

Now consider one of the full-dimensional polyhedra $X(v)$, and the trajectories $x(t)$ inside it. Let $X(v')$ be one of the faces of the polyhedron (i.e., $v'_i=0$ for some i, and $v'_j=v_j$, $j\neq i$). For given $\Delta(v)$, $\delta(v)$ and γ, there are three different options for the trajectories near $X(v')$ (see Figure 1):

(1) They are all exiting $X(v)$.
(2) They are all entering $X(v)$.
(3) Some trajectories are entering and some are exiting $X(v)$, or they are all parallel to $X(v')$.

The three options will lead to different approximating automata. An interesting question is now: How much could $\Delta(v)$, $\delta(v)$ and γ change, without changing the qualitative behaviour at each face of the polyhedron? Depending on how many of the parameters are varied simultaneously, this question may be more or less difficult to answer. If all of them are varied, the problem is a nonconvex quadratic problem (see Section 4.1). In the following section the question is answered for the case when $\gamma=0$, and in Section 4 the problem is solved for $\Delta(v)=0$. Only the two first options (all trajectories exit/enter $X(v)$) will be considered, since the solution sets of these problems will turn out to be the easiest to describe. The solution sets for the third option can be obtained as the complement of the union of the other solution sets.

It is easy to see that C_i is a normal vector of the polyhedron face $X(v')$. Using (2), the three cases from Figure 1 can be rewritten as

(1) $C_i[(A(v)-\Delta(v))x+b(v)-\delta(v)]>0$ for all $x\in X(v')$,
(2) $C_i[(A(v)-\Delta(v))x+b(v)-\delta(v)]<0$ for all $x\in X(v')$,
(3) $C_i[(A(v)-\Delta(v))x+b(v)-\delta(v)]=0$ for some $x\in X(v')$,

so the task is to find the sets of solutions (in $\Delta(v)$, $\delta(v)$ and γ) to all these problems. Rearranging the terms, e.g., the first problem can be written as

$$\begin{aligned} &C_i(A(v)x+b(v)) > C_i(\Delta(v)x+\delta(v)) \\ &\text{for all } x\in X(v') \end{aligned} \tag{5}$$

3. SOLUTIONS FOR SYSTEMS WITH KNOWN REGIONS

To begin with, let $\gamma = 0$. To get a solution to (5), a *direct representation* of $X(v')$ is needed:

$$X(v') = \{\sum_{j=1}^{r+h} \lambda_j x^j \mid \lambda_j \in \mathbb{R},\ \lambda_j \geq 0,\ \sum_{j=1}^{r} \lambda_j = 1\}$$

Here $x^j \in \mathbb{R}^n$, $j = 1,\ldots r$ are the corners of $X(v')$, and x^{r+j}, $j = 1,\ldots,h$, are vectors which are parallel to the unbounded edges of $X(v')$. When $X(v')$ is bounded, we have $h = 0$, and the direct representation means that each point of $X(v')$ is written as a convex combination of the corners.

For notational simplicity, let us drop the argument v of $A(v)$ etc. for a while. Now, the set of solutions to the problem is given by

$$S_{\Delta\delta} = \{(\Delta,\delta)\big| C_i(Ax^j + b) > C_i(\Delta x^j + \delta), \quad j = 1,\ldots,r;\ C_i A x^{r+j} \geq C_i \Delta x^{r+j},\ j = 1,\ldots,h\} \tag{6}$$

Proof. See (Roll, 2000).

Note that the solution set is a polyhedron in the space $\mathbb{R}^{n\times n} \times \mathbb{R}^n$, and therefore convex.

3.1 *Multiple requirements*

So far, only one single polyhedron face has been considered. In most cases, however, several transitions of an approximating automaton should remain invariant. This case is easily handled by partitioning the problem into subproblems of the form treated above, and then taking the intersection of the solution sets as the solution set for the entire problem. How many transitions needed to consider will depend on the system and what to verify. For example, if all that is needed is to keep the state on one side of a hyperplane, transitions through this hyperplane have to be considered. Note that considering fewer transitions will lead to a larger – and therefore less conservative – solution set, and will also require less computations.

4. SOLUTIONS FOR NON-FIXED REGIONS

The problem gets more complicated as soon as γ is not fixed anymore. One can immediately note that the regions $X(v)$ will no longer be fixed, but vary with γ. Also, several regions $X(v)$ have to be considered simultaneously, since moving a hyperplane will affect all regions adjacent to it. As mentioned in Section 2, only values of γ that keep the topology of the state-space regions invariant will be allowed. With this requirement, and with $\Delta(v) = 0$ for all v, the problem is still convex. However, some more notation is needed. First, note that each corner x^j of the full-dimensional polyhedron $X(v)$ is itself a region $X(v^j)$, where v^j contains (at least) n zeros. Here only the case when v^j has exactly n zeros will be treated; other cases can be regarded as degenerate special cases of this, with several corners in the same point.

Let $D_{[v^j]} = \text{diag}(v^j)$. Construct $Q_{[v^j]} \in \mathbb{R}^{(M-n)\times M}$ by deleting all rows in $D_{[v^j]}$ containing only zeros. Similarly, define $P_{[v^j]} \in \mathbb{R}^{n\times M}$ by deleting all rows in $I - D^2_{[v^j]}$ containing only zeros. Now $P_{[v^j]}$ has the following property: When multiplying another matrix from the left by $P_{[v^j]}$, it picks out the rows corresponding to the zero entries of v^j. $Q_{[v_j]}$, on the other hand, picks out the rows not picked out by $P_{[v^j]}$, and furthermore multiplies the rows corresponding to the -1 entries of v^j by -1.

With this notation, the equalities in (4) can be picked out by writing

$$P_{[v^j]} C x^j = P_{[v^j]}(d + \gamma)$$

Since x^j is uniquely determined by the equalities in (4), $P_{[v^j]}C$ will always be invertible. Hence,

$$x^j = (P_{[v^j]}C)^{-1} P_{[v^j]}(d + \gamma). \tag{7}$$

The demand that the topology should be preserved is the same as saying that it should always be possible to express each corner x^j as a region $X(v^j)$, where v^j must be constant. In other words, the equalities and inequalities (4) that define v^j should remain invariant. The equalities are satisfied by the construction of x^j in (7). Thus, the following set of inequalities are obtained for each corner $X(v^j)$ and all $i = 1,\ldots,M$:

$$C_i(P_{[v^j]}C)^{-1} P_{[v^j]}(d+\gamma) < d_i + \gamma_i \text{ if } v_i^j = -1$$
$$C_i(P_{[v^j]}C)^{-1} P_{[v^j]}(d+\gamma) > d_i + \gamma_i \text{ if } v_i^j = 1,$$

or more compactly

$$Q_{[v^j]} \left(C(P_{[v^j]}C)^{-1} P_{[v^j]} - I \right)(d+\gamma) \succ 0 \tag{8}$$

where $\succ$ denotes componentwise inequality.

What remains now is to take care of the requirements on the flow through the surfaces. This can be done completely analogously to Section 3, but with $\Delta = 0$. However, now the expression (7) has to be used in the inequalities of (6), yielding, e.g.,

$$\begin{aligned} &C_i(A(P_{[v^j]}C)^{-1} P_{[v^j]}(d+\gamma) + b) > C_i\delta, \\ &\qquad j = 1,\ldots,r; \\ &C_i A x^{r+j} \geq 0, \quad j = 1,\ldots,h \end{aligned} \tag{9}$$

for problem 1. Since the surfaces are only translated, the directions of the unbounded edges do not change, so x^{r+j} are not affected by γ. Inequalities like these, together with (8), give the final solution set. As can be seen, all inequalities are linear in δ and γ, and the resulting solution set is therefore a polyhedron.

4.1 Δ, δ *and* γ *are varied*

The final case, when all parameters are allowed to vary, is quite similar to the one when only Δ is fixed. Like above, the inequalities (8) are obtained. The requirements on the flow through the surfaces of a region are obtained by using (7) in (6):

$$C_i\Big((A-\Delta)(P_{[v^j]}C)^{-1}P_{[v^j]}(d+\gamma)+b-\delta\Big)>0, \quad j=1,\ldots,r;$$
$$C_iAx^{r+j}\geq C_i\Delta x^{r+j}, \;\; j=1,\ldots,h \qquad (10)$$

However, here the inequalities become quadratic, and the solution set is nonconvex. This makes it harder to efficiently represent and work with, and therefore this case will not be further discussed.

5. INTERPRETATIONS

Perhaps the most obvious interpretation is to view $\Delta(v)$, $\delta(v)$ and γ as uncertainties due to model errors and/or noise. Sections 3 and 4 then provide bounds for the uncertainties for the requirements of the approximating automata to hold. For natural reasons, the bounds may be very asymmetric, indicating that the system is more sensitive to certain types of model errors than to others.

The problem formulation is quite general in that no structure of $\Delta(v)$, $\delta(v)$ or γ is assumed. The only structure that is assumed is the topology of the different polyhedral regions $X(v)$. If the uncertainty has some further structure, $\Delta(v)$, $\delta(v)$ and γ can be parametrised accordingly, thereby reducing the dimensionality and simplifying the problem. For example, $\Delta(v)=0$ gives a model with additive noise.

An alternative interpretation is to consider $\Delta(v)$, $\delta(v)$ and/or γ as parameters of our choice, to be used for control design. One natural parametrisation would be $\gamma=0$, $\delta(v)=0$, $\Delta(v)=B(v)L(v)$, where $B(v)$ are fixed vectors, while $L(v)$ can be chosen freely. This gives (piecewise) linear state feedback control. Another parametrisation would be the one in Section 4, where γ can be regarded as a vector that lets us place the switching surfaces of a controller in an optimal manner.

6. EXAMPLE: A CHEMICAL REACTOR

To demonstrate the properties of this kind of problems, let us look at a simple example. In (Einarsson, 2000), a (fictional) chemical reactor is modelled, and a control strategy is proposed, after which some properties are verified. In this paper, bounds are computed for how large parameter uncertainties can be tolerated, and how much some of the control rules can be changed, before the verification is not valid any more.

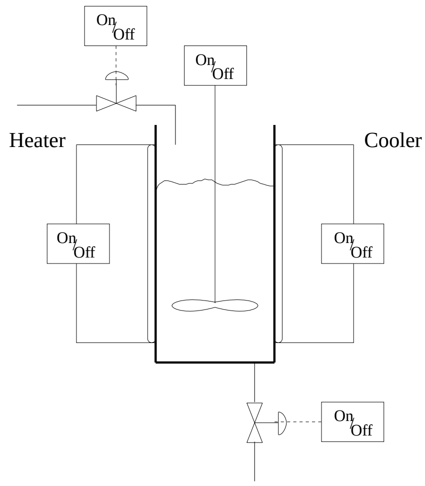

Fig. 2. A schematic figure of the chemical reactor

Table 1. Inputs to the chemical reactor

Signal	Interpretation
u_b	blender signal
u_i	inflow valve signal
u_d	draining valve signal
u_h	heater signal
u_c	cooler signal
u_r	reaction signal

6.1 *System model and requirements*

A figure of the chemical reactor is shown in Figure 2. It consists of a tank containing a mixture of two fluids. When a certain temperature is reached, a reaction between the fluids starts, giving the desired product. The temperature can be controlled by a heater and a cooler. There is also a blender helping to mix the fluid. The mixture is provided through an inflow valve. There is also a draining valve. The valves can be either open or closed.

The system model in (Einarsson, 2000) has two continuous state variables: the fluid level x_1 and the temperature x_2. There are also six control signals, each one taking a value in $\{0,1\}$. They are described in Table 1. u_r is an artificial, uncontrollable signal that indicates if the reaction is in progress. The plant dynamics is described by

$$\dot{x}=A(u)x+b(u) \qquad (11)$$

where

$$A(u)=10^{-3}\cdot\begin{bmatrix}-1.23u_\mathrm{d} & 0\\ 0 & -0.15-0.07u_\mathrm{b}\end{bmatrix}$$
$$b(u)=10^{-3}\cdot\begin{bmatrix}9838u_\mathrm{i}\\ 29.43u_\mathrm{h}+44.15(u_\mathrm{c}-u_\mathrm{r})\end{bmatrix}-$$
$$-\begin{bmatrix}\delta_\mathrm{h}u_\mathrm{i}\\ \delta_\mathrm{heat}u_\mathrm{h}+\delta_\mathrm{cool}u_\mathrm{c}+\delta_\mathrm{reac}u_\mathrm{r}\end{bmatrix}$$

Here the coefficients in $A(u)$ are assumed to be known, while the coefficients in $b(u)$ are uncertain.

The system is controlled according to the following rules, where $\gamma_1,\ldots,\gamma_5$ are design parameters:

(1) $u_\mathrm{b}=0$ when $x_1<3+\gamma_1$, $u_\mathrm{b}=1$ otherwise.

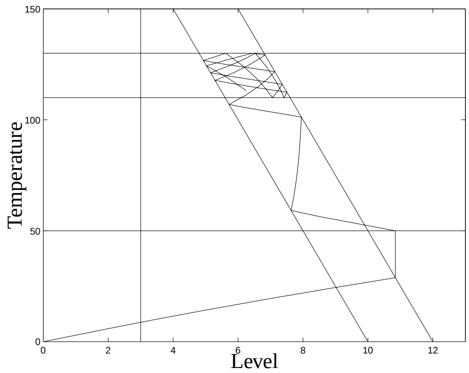

Fig. 3. The switching hyperplanes and an example trajectory.

(2) u_{i} is set to 0 when $25x_1 + x_2 = 300 + \gamma_3$, and is set to 1 when $25x_1 + x_2 = 250 + \gamma_2$.
(3) $u_{\mathrm{d}} = 0$ when $x_2 < 50$, $u_{\mathrm{d}} = 1$ otherwise.
(4) $u_{\mathrm{h}} = 1$ when $x_2 < 50$, $u_{\mathrm{h}} = 0$ otherwise.
(5) u_{c} is set to 0 when $x_2 = 110 + \gamma_4$, and is set to 1 when $x_2 = 130 + \gamma_5$.
(6) $u_{\mathrm{r}} = 0$ when $x_2 < 50$, $u_{\mathrm{r}} = 1$ otherwise.

The switching hyperplanes and a trajectory are shown in Figure 3. Note that the system contains hysteresis in u_{i} and u_{c}. This is handled by considering each polyhedron where the hysteresis occurs as two polyhedra with two different subsystems.

The requirements considered here are:

(1) Temperature should stay between 0 and 150.
(2) The tank must not be empty, and it must not overflow. The maximum level is 13.
(3) There should be an operating region with moderate temperature and fluid level which is invariant. In (Einarsson, 2000), this region is chosen to be $\{x \mid 250 \le 25x_1 + x_2 \le 300,\ 110 \le x_2 \le 130\}$. Here, the boundaries will also be affected by the values of γ.

These requirements can be translated to mathematical formulas:

(1) (a) $\dot{x}_2 > 0$ when $0 \le x_1 \le 13,\ \ x_2 = 0$.
(b) $\dot{x}_2 < 0$ when $0 \le x_1 \le 13,\ \ x_2 = 150$.
(2) (a) $\dot{x}_1 > 0$ when $x_1 = 0,\ \ 0 \le x_2 \le 150$.
(b) $\dot{x}_1 < 0$ when $x_1 = 13,\ \ 0 \le x_2 \le 150$.
(3) (a) $\dot{x}_2 > 0$ when $250 \le 25x_1 + x_2 \le 300$, $x_2 = 110$.
(b) $\dot{x}_2 < 0$ when $250 \le 25x_1 + x_2 \le 300$, $x_2 = 130$.
(c) $\begin{bmatrix} 25 & 1 \end{bmatrix} \dot{x} > 0$ when $25x_1 + x_2 = 250$, $110 \le x_2 \le 130$.
(d) $\begin{bmatrix} 25 & 1 \end{bmatrix} \dot{x} < 0$ when $25x_1 + x_2 = 300$, $110 \le x_2 \le 130$.

One also has to know what affine subsystems $\dot{x}$ will satisfy in the different cases, which is found by considering the control rules.

6.2 *Adjusting control rules*

Let us now try to find bounds, inside which the thresholds of the controller rules can be moved without affecting the properties to verify, i.e., how much the values of $\gamma_1, \ldots, \gamma_5$ can be changed.

The first requirement is to preserve the topology. Applying (8) to all corners yields the condition (after removing several redundant inequalities)

$$\begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 \\ 25 & -1 & 0 & 1 & 0 \\ 25 & -1 & 0 & 0 & 1 \\ 25 & -1 & 0 & 0 & 0 \\ 25 & 0 & -1 & 1 & 0 \\ 25 & 0 & -1 & 0 & 1 \\ 25 & 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & -1 \end{bmatrix} \gamma \prec \begin{bmatrix} 3 \\ 10 \\ 100 \\ 75 \\ 150 \\ 25 \\ 60 \\ 40 \\ 80 \\ 20 \\ 65 \\ 45 \\ 25 \\ 115 \\ 95 \\ 75 \\ 50 \\ 140 \\ 185 \\ 120 \\ 205 \\ 190 \\ 135 \\ 170 \\ 155 \\ 20 \end{bmatrix} \tag{12}$$

The first ten inequalities make sure that the moving hyperplanes do not pass any of the corners of the fixed hyperplanes (cf. Figure 3). The remaining inequalities state the relations between the moving hyperplanes (e.g., the last inequality means that the cooler should be turned off at a lower temperature than when it is turned on).

In addition to the topological requirement, the system also has to satisfy the properties to verify. This is achieved if the following inequalities, obtained from (9), are satisfied:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 25 & 0 & 0 & 1 & 0 & 0.0012 & 0 & -0.001 & 0 \\ 25 & 0 & 0 & 1 & 0 & 0.0012 & 0 & 0 & -0.001 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0.0002 & 0 \\ 25 & 0 & 1 & 1 & 0 & 0.0012 & 0 & -0.001 & 0 \\ 25 & 0 & 1 & 1 & 0 & 0.0012 & 0 & 0 & -0.001 \\ 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & -0.0002 \\ 0 & 0 & 0 & -1 & 0 & 0 & -0.0012 & 0.001 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & -0.0012 & 0 & 0.001 \\ 0 & 0 & -1 & -1 & 0 & 0 & -0.0012 & 0.001 & 0 \\ 0 & 0 & -1 & -1 & 0 & 0 & -0.0012 & 0 & 0.001 \end{bmatrix} \begin{bmatrix} \delta_{\mathrm{bh}} \\ \delta_{\mathrm{heat}} \\ \delta_{\mathrm{cool}} \\ \delta_{\mathrm{reac}} \\ \gamma_1 \\ \vdots \\ \gamma_5 \end{bmatrix}$$

$$\preccurlyeq \begin{bmatrix} 9.8380 \\ 0.0294 \\ 0.0225 \\ 245.7977 \\ 245.8179 \\ 0.0200 \\ 245.7536 \\ 245.7738 \\ 0.0286 \\ 0.2138 \\ 0.1935 \\ 0.2579 \\ 0.2377 \end{bmatrix} \tag{13}$$

Together with (12), (13) now describes the region, in which the values of δ_{bh}, δ_{heat}, δ_{cool}, δ_{reac}, and γ are allowed to vary.

From (13), one can go further and, e.g., find the values of γ that allow as large uncertainties as possible in the b parameters. This gives in a sense the maximally robust controller satisfying the verification, and is calculated similarly to the computation of the *Chebychev centre* of a polyhedron (the centre of the largest sphere inscribed in a polyhedron (see Boyd and Vandenberghe, 1999)). What should be computed here is the largest disc, parallel to the γ coordinate axes and with its centre somewhere along the subspace $\delta = 0$, inscribed in the polyhedron defined by (12) and (13). Represent the disc as

$$\mathscr{D} = \{ \begin{bmatrix} 0 \\ \gamma \end{bmatrix} + \begin{bmatrix} \delta \\ 0 \end{bmatrix} \mid \|\delta\| \leq R \} \tag{14}$$

where the vector $\left[\begin{smallmatrix} 0 \\ \gamma \end{smallmatrix}\right]$ is the centre of the disc and R is the radius. Now R should be maximised, subject to the constraint that $\mathscr{D}$ satisfies (12) and (13). Stack (12) and (13) on top of each other, and denote the resulting matrices according to

$$F \begin{bmatrix} \delta \\ \gamma \end{bmatrix} \preccurlyeq g \tag{15}$$

For each row i in (15), the constraint that $\mathscr{D}$ should satisfy $F_i \left[\begin{smallmatrix} \delta \\ \gamma \end{smallmatrix}\right] \leq g_i$ can be expressed

$$F_i \begin{bmatrix} 0 \\ \gamma \end{bmatrix} + \sup_{\|\delta\| \leq R} F_i \begin{bmatrix} \delta \\ 0 \end{bmatrix} \leq g_i$$

But since

$$\sup_{\|\delta\| \leq R} F_i \begin{bmatrix} \delta \\ 0 \end{bmatrix} = \sup_{\|\delta\| \leq R} F_i \begin{bmatrix} I \\ 0 \end{bmatrix} \delta = R \left\| F_i \begin{bmatrix} I \\ 0 \end{bmatrix} \right\|$$

(where I is an identity matrix with the same number of rows as δ), it follows that

$$F_i \begin{bmatrix} 0 \\ \gamma \end{bmatrix} + R \left\| F_i \begin{bmatrix} I \\ 0 \end{bmatrix} \right\| \leq g_i$$

This is a linear inequality in γ and R, and the desired value of γ can be computed from the LP

$$\max_{\gamma, R} R$$
$$\text{subj. to } F_i \begin{bmatrix} 0 \\ \gamma \end{bmatrix} + R \left\| F_i \begin{bmatrix} I \\ 0 \end{bmatrix} \right\| \leq g_i, \; i = 1, \ldots, M_F$$

where M_F is the number of rows of F.

7. CONCLUSIONS

This paper presents an approach to investigate how sensitive approximating automata for piecewise affine systems, as described in (Einarsson, 2000), might be to changes in the underlying subsystems and to translations of the switching surfaces. Sections 3 and 4 provided the sets of system matrices that satisfy certain demands on the behaviour of the system. As pointed out, these can either be seen as giving a measure of how robust the approximating automata are to uncertainties in the system, or as giving limits for how much the system can be changed, e.g., in a control design process, without altering the overall behaviour described by the approximating automata.

It would be natural to combine these demands with other objectives. One example of this was given in Section 6.2. To give another example, when using the state feedback parametrisation described in Section 5, one would probably want to find $L(v)$ that are optimal in a certain respect. Since the solution sets of the two first problems in Sections 3 and 4 are convex, all sorts of convex optimisation problems can be formed, which can be solved efficiently once the direct representations of the polyhedra are known (see Boyd and Vandenberghe, 1999).

The theory in this paper is immediately extendible to switched systems as described in (Einarsson, 2000). The important thing is that the switch sets are hyperplanes in the state space.

8. REFERENCES

Alur, R., T. A. Henzinger, G. Lafferriere and G. J. Pappas (2000). Discrete abstractions of hybrid systems. *Proceedings of the IEEE* **88**(7), 971–984.

Bemporad, A., F. D. Torrisi and M. Morari (2000). Optimization-based verification and stability characterization of piecewise affine and hybrid systems. In: *Hybrid Systems: Computation and Control*. Vol. 1790 of *Lecture Notes in Computer Science*. Springer-Verlag. pp. 45–58.

Boyd, S. and L. Vandenberghe (1999). Convex optimization. Course Reader for EE364, Introduction to Convex Optimization with Engineering Applications, Stanford Univ.

Chutinan, A. (1999). Hybrid System Verification Using Discrete Model Approximations. PhD thesis. Dept. of Electrical and Computer Engineering, Carnegie Mellon Univ.

Einarsson, V. (2000). Model Checking Methods for Mode Switching Systems. PhD thesis. Dept. of Electrical Engineering, Linköping Univ. SE-581 83 Linköping, Sweden.

Engell, S., S. Kowalewski, C. Schulz and O. Stursberg (2000). Continuous-discrete interactions in chemical processing plants. *Proceedings of the IEEE* **88**(7), 1050–1068.

Johansson, M. (1999). Piecewise Linear Control Systems. PhD thesis. Dept. of Automatic Control, Lund Institute of Technology, Lund Univ. Box 118, SE-221 00 Lund, Sweden.

Roll, J. (2000). Invariance of approximating automata for piecewise linear systems with uncertainties. In: *Hybrid Systems: Computation and Control*. Vol. 1790 of *Lecture Notes in Computer Science*. Springer-Verlag. pp. 396–406.