Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

A Barrier Certificate Approach to the Verification of the Safe Operation of a Chemical Reactor

G. A. Shah *; **M. Völker** *; **C. Sonntag** *; **S. Engell** *

* *Process Dynamics and Operations Group, Dept. of Bio- and Chemical Engg., TU Dortmund, Germany (Tel: +49-0231-755 5342; e-mail: {gaurang.shah,marten.voelker,christian.sonntag,sebastian.engell}@bci.tu-dortmund.de).*

Abstract: In industrial practice, extensive simulations are performed in order to analyse the safety and the correct operation of controlled chemical processes. One aspect of verifying the safe operation is to prove that the states of the system stay within a safe region for a certain set of inputs or disturbances which is the main theme of this paper. Recently, a rigorous method for this type of verification problem has been proposed which makes use of *Barrier Certificates* for verifying whether an undesired set of states can be reached. If the system dynamics can be described in *polynomial* form, the safety of the system can be proven algorithmically. The determination of a barrier certificate is a sum-of-squares (SOS) problem which can further be transformed into a non-convex Bilinear Matrix Inequality (BMI) problem. This paper deals with proving the safety of a Continuously Stirred Tank Reactor (CSTR), a non-linear system, using barrier certificates. Uncertainties are represented by a bounded disturbance acting on the system. Safety is explicitly proven for a convex set of initial conditions and a non-convex unbounded unsafe set. Two situations are considered, the uncontrolled plant and the closed-loop system with a state-feedback controller. For the solution of the BMI problem, three different numerical approaches are compared. It turned out that solving the non-convex BMI problem directly is more efficient than solving it using the convex iterative approach.

Keywords: Barrier certificate, Nonlinear systems, Chemical reactor, Polynomial methods, Polynomial models, Safety analysis.

1. INTRODUCTION

In industrial practice, the validation of a controller is usually performed by simulations of the closed-loop system. However, with this method not all uncertainty scenarios can be examined which implies that the success of a controller at a real plant depends on the correct choice of the simulation parameters, e.g. the disturbances and the parametric model uncertainties. As a result, guarantees for the performance of a controller cannot be given. A possibility to rigorously certify the stability and the reachability of the system is the construction of auxiliary functions as e.g. Lyapunov functions [Khalil (1996)] or *Barrier Certificates* [Prajna and Jadbabaie (2004)]. While for the analysis of linear systems, quadratic Lyapunov functions and theorems from robust linear control are sufficient, there exists no algorithmic procedure for the construction of Lyapunov functions or Barrier Certificates for general uncertain nonlinear systems. In certain cases, a systematic construction of such functions can be performed, especially for low-order non-linear models. The polynomial description of systems provides a suitable basis for the algorithmic construction of such auxiliary functions and by suitable transformations, an even larger class of non-linear systems can also be examined [Papachristodoulou and Prajna (2005)], [Savageau and Voit (1987)]. For polynomial systems, a suitable set of parameterized polynomial Lyapunov functions or Barrier certificates can be constructed using the sum-of-squares (SOS) decomposition and the Positivstellensatz, a theorem from real-algebraic geometry [Parrilo (2000)], [Stengle (1974)]. The Positivstellensatz can be considered as a generalization of the S-procedure [Boyd et al. (1994)] used in robust control theory where the positivity of a quadratic polynomial function over a quadratic set is proven using constant multipliers, usually introducing a certain amount of conservativeness. The Positivstellensatz proves the positivity of a polynomial function over a set of polynomial constraints using parameterized polynomial multipliers which can be evaluated with the help of numerical optimization techniques. However, this often leads to bilinear representations that contain products of two unknown coefficients. Such bilinear representations cannot be represented as convex Linear Matrix Inequalities (LMIs), but lead to Bilinear Matrix Inequalities (BMIs) which may be non-convex. Non-convex problems are difficult to solve in general since there may be many local optima. By introducing additional variables, known as the *lifting* variables, it is possible to transform BMIs into LMI problems. Similarly, a product of more than two unknown coefficients in a polynomial leads to general Polynomial Matrix Inequality (PMI) problems which can also be trans-

formed into LMI problems. However, it is difficult to assess the conservativeness of such transformations.

Using Lyapunov functions, one can indirectly prove system safety by proving asymptotic stability globally or locally (within a region of attraction). The determination of a Lyapunov function for non-linear systems can also be done systematically using SOS decompositions [Papachristodoulou and Prajna (2002)]. However, a drawback of the Lyapunov function approach is that it requires the stronger result that the system is exponentially stable in the region of attraction.

This paper deals with the safety verification of a nonlinear polynomial system. The system is considered to be safe if its trajectories always stay within a bounded region for a given bounded set of disturbances. The theoretical contribution of this paper is the consideration of an unbounded non-convex unsafe set which has so far not been treated in the literature. We use the method to verify the system safety for a Continuously Stirred Tank Reactor (CSTR) [Klatt and Engell (1998)] with the van-der-Vusse reaction scheme by determining a smallest possible reachable region around the operating point of the system. Using barrier certificates, the safety of the system is proven for the uncontrolled (open-loop) case as well as for the controlled (closed-loop) case. The bilinear SOS problem is solved by alternatingly fixing the optimization degrees of freedom and solving the resulting convex LMI problems repeatedly [Prajna and Jadbabaie (2004)] as well as by the penalty method from [Stingl (2005)]. For our problem, the penalty method is more efficient.

2. PRELIMINARIES

2.1 Mathematical Notations

We denote a scalar variable by lowercase characters, vectors by lowercase bold characters and $n \times m$ matrices by uppercase bold characters. Let $\mathcal{S}^n$ denote a set of symmetric matrices of size $n \times n$, $\mathcal{X}$ denote a set of all possible values of the states of the system and $\mathcal{D}$ a set of possible disturbance values. We use subscripts 0, u and d for representating initial, unsafe and disturbance sets respectively. The symbol $\succeq$ indicates positive semidefiniteness of a matrix. The complement of a set is indicated by using $\perp$ as a superscript. $\mathbb{N}_0$ is a set of natural numbers. $\mathbb{R}$ and $\mathbb{C}$ denote real and complex vector spaces respectively.

2.2 Sum-of-Squares Decomposition

A polynomial $p(x)$ of degree $2d$ can be shown to be non-negative or a sum-of-squares (SOS) if it can be shown that $p(x) = \mathbf{Z}(x)^T \mathbf{Q} \mathbf{Z}(x)$ where $\mathbf{Q} \succeq 0$ and $\mathbf{Z}(x)$ is a monomial vector in x of degree $\leq d$ [Parrilo (2000)]. If $p(x) = \sum_i c_i x^{\boldsymbol{\alpha}_i}$, $\boldsymbol{\alpha}_i \in \mathbb{N}_0$, that is $p(x)$ is affine in an unknown coefficient vector (also known as the decision variable) $\mathbf{c} = [c_1\ c_2\ c_3\ \ldots]^T$, then proving non-negativity of $p(x)$ is a convex semidefinite program in $\mathbf{c}$ and $\mathbf{Q}$:

$$p(x) \geq 0 \Leftrightarrow\ \exists\, \mathbf{c}, \mathbf{Q} :\ \mathbf{Q} \succeq 0,\ \text{trace}(\mathbf{A}_i \mathbf{Q}) = c_i, \quad (1)$$

where $\mathbf{A}_i$ is a real matrix of suitable dimension that is determined from the comparision of the coefficients of $p(x)$ and $\mathbf{Z}(x)^T \mathbf{Q} \mathbf{Z}(x)$. Determining $\mathbf{Q} \succeq 0$ is an LMI problem.

Note that, with the above formulation, $p(x) \geq 0$ is proved independent of the range of the variable x. Therefore, x is also called the independent variable. The following is an example of a SOS decomposition:

$$\begin{aligned} p(\mathbf{x}) &= 2x_1^4 + 5x_2^4 + 2x_1^3 x_2 - x_1^2 x_2^2 \\ &= \begin{bmatrix} x_1^2 & x_2^2 & x_1 x_2 \end{bmatrix} \begin{bmatrix} 2 & -3 & 1 \\ -3 & 5 & 0 \\ 1 & 0 & 5 \end{bmatrix} \begin{bmatrix} x_1^2 \\ x_2^2 \\ x_1 x_2 \end{bmatrix} \\ &= \frac{1}{2}(2x_1^2 - 3x_2^2 + x_1 x_2)^2 + \frac{1}{2}(x_2^2 + 3x_1 x_2)^2. \end{aligned} \quad (2)$$

The SOS decomposition of the product between two parameterized polynomials $p(x)$ and $q(x)$ is a non-convex semidefinite program which is referred to as a Bilinear Matrix Inequality (BMI):

$$\begin{aligned} &p(x) \cdot q(x) \geq 0 \Leftrightarrow\ \exists\, \mathbf{c}, \mathbf{d}, \mathbf{Q} : \\ &\mathbf{Q} \succeq 0,\ \text{trace}(\mathbf{A}_{ij} \mathbf{Q}) = c_i d_j, \end{aligned} \quad (3)$$

where $\mathbf{A}_{ij}$ is determined similar to $\mathbf{A}_i$ as described above. BMI or, in general, PMI problems are difficult to solve because of their non-convex solution set. Some approaches to solve such problems are discussed in section 3.2.

2.3 Positivstellensatz

In control theory, it is often required to prove the satisfaction of some condition only when other condition(s) are fulfilled. For example, consider that we have polynomial functions $p(x)$, $\mathbf{g}(x)$ and $\mathbf{h}(x)$ that it is required to prove that,

$$p(x) \geq 0 \ \text{ whenever } \mathbf{g}(x) \geq 0,\ \mathbf{h}(x) = 0,\ x \in \mathbb{R}. \quad (4)$$

Alternatively, we may want to prove that the intersection of the sets $p(x) \geq 0$, $\mathbf{g}(x) \geq 0$ and $\mathbf{h}(x) = 0$ is non-empty in $\mathbb{R}$. The above requirement can be proven using the Positivstellensatz. The Positivstellensatz is an algebraic technique [Parrilo (2000)], [Stengle (1974)] which combines a set of inequality and equality constraints into a single inequality constraint. The individual conditions in (4) can be combined by using multipliers:

$$\begin{aligned} &p(x) - \boldsymbol{\sigma}^T(x) \mathbf{g}(x) + \boldsymbol{\lambda}^T(x) \mathbf{h}(x) \geq 0, \\ &\sigma_i(x) \geq 0,\ \forall\, i,\ x \in \mathbb{R}, \end{aligned} \quad (5)$$

where $\sigma_i(x) = \sum_j s_j x^{\boldsymbol{\alpha}_j}$, $\lambda_i(x) = \sum_j l_j x^{\boldsymbol{\alpha}_j}$, $\boldsymbol{\alpha}_j \in \mathbb{N}_0$. $\sigma_i(x)$ and $\lambda_i(x)$ are multiplier polynomials affine in the unknown coefficients s_j and l_j. Thus, if such $\boldsymbol{\sigma}(x)$ and $\boldsymbol{\lambda}(x)$ exist, then we are able to prove (4). Inequality (5) is affine in the unknown coefficients of $\boldsymbol{\sigma}(x)$, $\boldsymbol{\lambda}(x)$ and therefore is an LMI problem.

Thus, it can be seen that, using the Positivstellensatz, we are able to prove the non-negativity of a polynomial over a semialgebraic set (a set of equalities and inequalities). Using multipliers, the problem can be transformed into a convex one.

2.4 Barrier Certificates

A barrier certificate is a polynomial function of the states of a system which, if it exists, proves the safety of the system [Prajna and Jadbabaie (2004)]. Consider a continuous dynamic system

$$\dot{\mathbf{x}} = f(\mathbf{x}),\ \mathbf{x} \in \mathcal{X}. \quad (6)$$

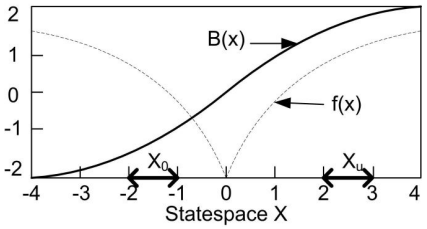


Fig. 1. Idea of a Barrier certificate.

Let $\mathcal{X}_0$ be an initial set of states and $\mathcal{X}_u$ be an unsafe set of states. Then, a barrier certificate $B(\mathbf{x})$ satisfies the following requirements:

$$B(\mathbf{x}) > 0 \; \forall \, \mathbf{x} \in \mathcal{X}_u, \tag{7}$$

$$B(\mathbf{x}) \leq 0 \; \forall \, \mathbf{x} \in \mathcal{X}_0, \tag{8}$$

$$\frac{\partial B}{\partial x}(\mathbf{x}) f(\mathbf{x}) \leq 0 \; \forall \, \mathbf{x} \text{ when } B(\mathbf{x}) = 0. \tag{9}$$

The basic idea is to require that $B(\mathbf{x})$ is strictly positive in $\mathcal{X}_u$ and non-positive in $\mathcal{X}_0$ (see Fig. (1)). The third requirement (9) ensures that, at $B(\mathbf{x}) = 0$, the rate of change of $B(\mathbf{x})$ along the flow of system dynamics is always non-increasing. This ensures that the system trajectories will never cross the zero-level set. Hence, $B(\mathbf{x}) = 0$ serves as a barrier between $\mathcal{X}_0$ and $\mathcal{X}_u$. Employing the Positivstellensatz, the requirements (7)-(9) can be treated as SOS constraints if the function $f(\mathbf{x})$ is polynomial.

3. MAIN IDEA

3.1 Problem Definition

We consider the following system:

$$\begin{aligned} &\dot{\mathbf{x}}(t) = f(\mathbf{x}(t), \mathbf{u}(t), \mathbf{d}(t)), \\ &\mathbf{x}(t) \in \mathcal{X} \subseteq \mathbb{R}^{n_x}, \; \mathbf{d}(t) \in \mathcal{D}_d \subseteq \mathbb{R}^{n_d}, \end{aligned} \tag{10}$$

where $\mathbf{u}(t) = \mathbf{K}\mathbf{x}(t)$ is the control input and $\mathbf{d}(t)$ is a disturbance variable. We assume $\mathbf{x} = 0$, $\mathbf{u} = 0$ and $\mathbf{d} = 0$ as the nominal operating point. Given an initial set, our goal is to determine a barrier function around the operating point which serves as an upper bound on the maximum reachability set of the system. The barrier certificate problem for the disturbed system (10) is then given by:

$$\begin{aligned} &B(\mathbf{x}) > 0 \; \forall \, \mathbf{x} \in \mathcal{X}_u, \\ &B(\mathbf{x}) \leq 0 \; \forall \, \mathbf{x} \in \mathcal{X}_0, \\ &\frac{\partial B}{\partial x}(\mathbf{x}) f(\mathbf{x}, \mathbf{u}, \mathbf{d}) \leq 0 \; \forall \, \mathbf{x} \text{ when } B(\mathbf{x}) = 0, \; \mathbf{u} = \mathbf{K}\mathbf{x}, \; \mathbf{d} \in \mathcal{D}_d. \end{aligned} \tag{11}$$

The initial set $\mathcal{X}_0$ is fixed as a convex ellipsoid with parameter r_0:

$$\begin{aligned} &\mathcal{X}_0 = \{\mathbf{x} \in \mathcal{X} | g_0(\mathbf{x}) \geq 0\}, \; g_0(\mathbf{x}) = \mathbf{x}^T(-\mathbf{P}_0)\mathbf{x} + r_0^2, \\ &\mathbf{P}_0 \succeq 0. \end{aligned} \tag{12}$$

The unsafe set $\mathcal{X}_u$ is parameterized by an unknown radius r_u as:

$$\begin{aligned} &\mathcal{X}_u = \{\mathbf{x} \in \mathcal{X} | g_u(\mathbf{x}) \geq 0\}, \; g_u(\mathbf{x}) = \mathbf{x}^T(\mathbf{P}_u)\mathbf{x} - r_u^2, \\ &\mathbf{P}_u \succeq 0. \end{aligned} \tag{13}$$

Therefore, $\mathcal{X}_u$ is an unbounded non-convex set. If (11) holds, $\mathcal{X}_u$ is the set of states that cannot be reached. Thus, its complement $\mathcal{X}_u^{\perp}$ is a superset of all reachable states.

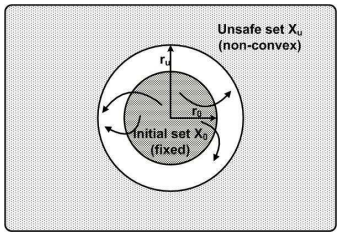


Fig. 2. Illustration of the problem: The goal is to minimize r_u. The curved arrows represent possible trajectories.

That is, $\mathcal{X}_u^{\perp} \supseteq \mathcal{X}_0$. The disturbance set is $\mathcal{D}_d = \{\mathbf{d} | g_d(\mathbf{d}) \geq 0\}$ where $g_d(\mathbf{d})$ is defined polynomially.

Our objective is to determine $B(\mathbf{x})$ for the maximum unsafe set or equivalently for the minimum reachable set. In other words, we search for the minimum radius r_u (see Fig. (2)). We restrict our search for r_u to a compact subset of the statespace $\mathcal{X}_{ss} \in \mathcal{X}$, characterized by $\mathcal{X}_{ss} = \{\mathbf{x} \in \mathcal{X} | g_{ss}(\mathbf{x}) \geq 0\}$. By choosing $\mathcal{X}_{ss}$ large enough, this does not impose an additional restriction but it facilitates the numerical solution. From the definitions of the sets $\mathcal{X}_0$, $\mathcal{X}_u$ and $\mathcal{D}_d$ and the definition of the barrier certificate (11), the following SOS optimization problem is obtained employing the Positivstellensatz (5):

$$\begin{aligned} &\min r_u \text{ subject to:} \\ &SOS1: B(\mathbf{x}) - \epsilon - \sigma_u(\mathbf{x}) g_u(\mathbf{x}) - \sigma_{ss}(\mathbf{x}) g_{ss}(\mathbf{x}) \geq 0, \\ &SOS2: -B(\mathbf{x}) - \sigma_0(\mathbf{x}) g_0(\mathbf{x}) - \sigma_{ss}(\mathbf{x}) g_{ss}(\mathbf{x}) \geq 0, \\ &SOS3: -\frac{\partial B}{\partial x}(\mathbf{x}) f(\mathbf{x}, \mathbf{u}, \mathbf{d}) - \sigma_{ss}(\mathbf{x}) g_{ss}(\mathbf{x}) - \\ &\qquad \sigma_d(\mathbf{d}) g_d(\mathbf{d}) + \lambda_B(\mathbf{x}, \mathbf{d}) B(\mathbf{x}) \geq 0, \\ &SOS4\text{–}SOS7: \sigma_u(\mathbf{x}) \geq_{SOS} 0, \; \sigma_0(\mathbf{x}) \geq 0, \\ &\qquad \sigma_{ss}(\mathbf{x}) \geq_{SOS} 0, \; \sigma_d(\mathbf{d}) \geq 0, \end{aligned} \tag{14}$$

where σ, λ are the multipliers that are parameterized affinely in unknown coefficients and ϵ is a small positive constant which ensures strict positivity of $B(\mathbf{x})$ in $\mathcal{X}_u$. The set of inequalities (14) involves products between the unknown coefficients due to terms $\sigma_u(\mathbf{x}) g_u(\mathbf{x})$ and $\lambda_B(\mathbf{x}, \mathbf{d}) B(\mathbf{x})$. Hence, problem (14) is a BMI problem. The following section discusses approaches to solve BMI problems.

3.2 Some Approaches to Solve BMI Problems

We solve the bilinear optimization problem (14) here using the three different methods:

(i) Iterative approach

This approach is adapted from [Prajna and Jadbabaie (2004)]. Consider again equation (3) which involves a product between the coefficients $\mathbf{c}$ and $\mathbf{d}$. In this approach, the BMI problem is solved by alternatingly fixing $\mathbf{c}$ and $\mathbf{d}$. Fixing either of them at a time leads to convex LMI problems. Below, we state the algorithm that implements this approach for problem (14):

Algorithm 3.1. (1) **Initialization**: In this step, $B(\mathbf{x})$ and $\mathcal{X}_u$ (that is, the radius r_u) are initialized. It is easier to initialize $B(\mathbf{x})$ rather than $\lambda_B(\mathbf{x}, \mathbf{d})$ since one can always assume a circular $B(\mathbf{x})$ separating $\mathcal{X}_0$ and $\mathcal{X}_u$. Also, a very small $\mathcal{X}_u$ is chosen; that is r_u is chosen very large such that it lies at the mid-point of a chosen interval.

$$r_u = (lb + ub)/2, \tag{15}$$

where lb, ub denote the lower bound and the upper bound of the interval respectively. The optimization problem (14) is solved to determine a feasible $\lambda_B(\mathbf{x}, \mathbf{d})$ and other multipliers.

If the problem is infeasible, then r_u is increased using a *bisection* method in which,

$$lb = r_u,\ r_u = (lb + ub)/2. \tag{16}$$

If the problem is feasible, then r_u is decreased using a bisection method in which,

$$ub = r_u,\ r_u = (lb + ub)/2. \tag{17}$$

The optimization is repeated until a minimum value of r_u is obtained. This step can be described as:

solve (14) for a fixed $B(\mathbf{x})$.

(2) **Fixing** $\lambda_B(\mathbf{x}, \mathbf{d})$: The feasible solution $\lambda_B(\mathbf{x}, \mathbf{d})$ obtained from the previous step is fixed. Starting from the minimum r_u obtained in the previous step, the optimization problem is solved to determine a feasible $B(\mathbf{x})$ and a new minimum r_u which is lower than the one obtained in the previous step. During the course of optimization, r_u is varied by the bisection method (15)-(17). This step can be described as:

solve (14) for a fixed $\lambda_B(\mathbf{x}, \mathbf{d})$.

(3) **Fixing** $B(\mathbf{x})$: The feasible $B(\mathbf{x})$ obtained from the previous step is fixed. Starting from the minimum r_u obtained in the previous step, this step is same as the step (1). On obtaining a new minimum r_u, goto step (2) and the whole procedure is repeated until a stopping criterion is satisfied.

(ii) Theory of Moments approach

The theory of moments method is based on the *lifting and relaxation* technique [Lasserre (2001)]. Lifting is required to replace the bilinear terms by a single variable so that the resulting inequality can be represented in LMI form. For example, consider the following BMI problem:

$$p + q + p \cdot q \geq 0;\ p, q \in \mathbb{R}. \tag{18}$$

Replacing each monomial $p^i q^j$ with a *lifting* variable y_{ij}, inequality (18) can be written as,

$$y_{10} + y_{01} + y_{11} \geq 0. \tag{19}$$

The lifting variables satisfy the following non-convex constraints:

$$y_{10} \cdot y_{01} = y_{11},\ y_{20} = y_{10}^2,\ y_{02} = y_{01}^2. \tag{20}$$

The non-convex constraints can be *relaxed* by building a *moment matrix* of first order, thereby relaxing monomials of degree up to 2, as follows:

$$M_1(\mathbf{y}) = \left[\begin{array}{c|cc} 1 & y_{10} & y_{01} \\ \hline y_{10} & y_{20} & y_{11} \\ y_{01} & y_{11} & y_{02} \end{array}\right] \succeq 0. \tag{21}$$

Inequalities (19)+(21) constitute an LMI problem. Owing to the relaxation, the feasible solution set of the original non-convex problem is enlarged and is also convex. Solution of the relaxed problem gives an upper bound on the global optimum solution of the original problem (18). Further relaxation would introduce additional variables resulting in additional constraints which would further reduce the feasible convex solution set (obtained from the previous LMI relaxation), thereby making the relaxation *tighter*. This results in a reduction of the gap between the global optimum and the relaxed optimum. Building a nested series of LMI relaxations, the method converges towards the global optimum. The following scheme represents the idea of the method:

$$\mathrm{Sol}_{LMI_1} \supset \mathrm{Sol}_{LMI_2} \supset \ldots \supset \mathrm{Sol}_{BMI\,problem},$$
$$\text{tighter relaxation} \longrightarrow$$

where Sol_{LMI_1} is the convex solution set of the 1^{st}-order LMI relaxation and so on. The size of the relaxed LMI problem grows polynomially with the relaxation order. Therefore, the approach requires a large memory and is computationally expensive.

(iii) Penalty/Augmented Lagrangian approach

Penalty/Augmented Lagrangian methods are similar to the *interior-point* (IP) methods [Nesterov and Nemirovsky (1994)] which are useful in solving convex optimization problems like the LMI problems. The penalty/augmented Lagrangian method differs from the IP method in that the former makes use of the *penalty* function which penalizes the matrix inequality constraints. With some internal change of variables and matrix operations, the method can be extended to BMI problems as well. This method requires a starting point for its initialization which can be fixed to zero in most cases. A detailed discussion on this method and on the choice of a suitable penalty function can be found in [Stingl (2005)].

The computational complexity of this method is dominated by the construction of the Hessian (second-order derivative) of the augmented Lagrangian. The efficiency of the algorithm can be considerably improved by exploiting the sparse structure of the Hessian matrix. The penalty/augmented Lagrangian method only guarantees local convergence. When initialized appropriately, the convergence to the optimum solution is fast.

To implement the iterative approach, SOSTOOLS (available at www.cds.caltech.edu/sostools/) along with SeDuMi [Sturm (1999)], both are freely available MATLAB [1] -based toolboxes, were used. For implementing the theory of moments, YALMIP [Löfberg (2004)] along with SOLVEMOMENT (shipped freely with YALMIP), which are also freely available toolboxes, were used. For implementing the penalty/augmented Lagrangian method, YALMIP along with PENBMI (see www.penopt.com/ for a free developer version) were used.

4. CASE STUDY: A CSTR SYSTEM

A Continuous Stirred Tank Reactor (CSTR) system is considered [Klatt and Engell (1998)] with the van-der-Vusse reaction scheme:

$$A \overset{k_1}{\rightarrow} B \overset{k_2}{\rightarrow} C,\ \text{and}\ 2A \overset{k_3}{\rightarrow} D,$$

where A is the educt, B is the product, C and D are the unwanted by-products, and k_1, k_2, k_3 are the reaction rates. The original model (see Fig.(3)) is a 4^{th}-order non-linear ordinary differential equation (ODE) system containing

[1] A registered trademark of The MathWorks, Inc.

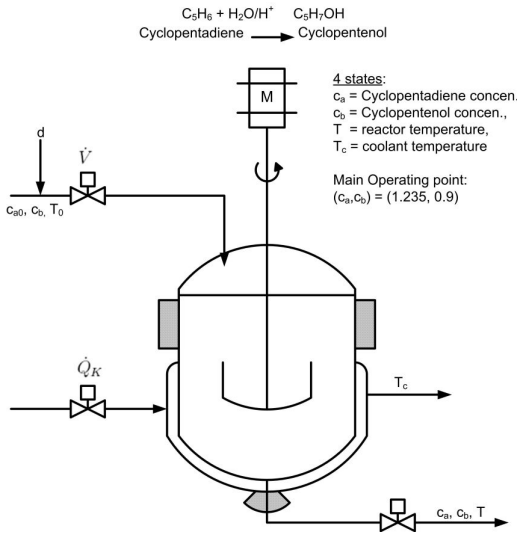


Fig. 3. Continuously stirred tank reactor.

exponential terms in the rate coefficients k_1, k_2, k_3. Assuming tight temperature control, the exponential terms can be approximated by constants and the model can be simplified to a 2^{nd}-order non-linear ODE system:

$$\begin{aligned}\frac{dc_a}{dt} &= 0.0999 \cdot \dot{V} \cdot (c_{a0} + d - c_a) - 0.01450 \cdot c_a \\ &\quad - 1.92861 \cdot 10^{-03} \cdot c_a^2, \\ \frac{dc_b}{dt} &= -0.0999 \cdot \dot{V} \cdot c_b + 0.01450 \cdot c_a - 0.01450 \cdot c_b.\end{aligned} \tag{22}$$

where c_a, c_b are the concentrations of the educt and the product, respectively, $\dot{V}$ is the input flow rate of educt A and is the manipulated variable, c_{a0} is the nominal input concentration of educt A, and d is the disturbance acting on the input concentration c_{a0}.

Here, $c_{a0} = 5.1$ mol/l. The nominal operating point is $c_a = 1.235$ mol/l, $c_b = 0.9$ mol/l and $\dot{V} = 0.05236$ l/s. The practical limits of the state space $\mathcal{X}_{ss}$ are as follows:

$$\begin{aligned}c_{amin} = 0 \text{ mol/l}, \; c_{amax} = 14.09 \text{ mol/l}, \\ c_{bmin} = 0 \text{ mol/l}, \; c_{bmax} = 11.07 \text{ mol/l}.\end{aligned} \tag{23}$$

Therefore, we have the following state space constraints:

$$\begin{aligned}g_{ss}(c_a) = (c_a - 0)(14.09 - c_a) \geq 0, \\ g_{ss}(c_b) = (c_b - 0)(11.07 - c_b) \geq 0.\end{aligned} \tag{24}$$

As concentrations cannot become negative, $d \geq -5.1$ mol/l. We restrict d to the relatively large range -1.8708 mol/l $\leq d \leq 1.8708$ mol/l. Therefore, the disturbance set is given by

$$g_d(d) = -d^2 + 1.8708^2 \geq 0. \tag{25}$$

For reasons of numerical stability, we perform *shifting* and *scaling* of system (22) along with the constraints. The nominal operating point of the system is shifted to the origin and the whole system is scaled so that the values of the state variables vary between -1 and $+1$. The transformed variables are given by,

$$\begin{aligned}x_1 = \frac{c_a - 1.235}{14.09 - 0}, \; x_2 = \frac{c_b - 0.9}{11.07 - 0}, \\ x_d = \frac{d - 0}{1.8708 - (-1.8708)}, \; u = \dot{V} - 0.05236.\end{aligned}$$

The initial set is fixed as a convex set around the nominal operating point, that is

$$\begin{aligned}g_0(\mathbf{x}) &= \mathbf{x}^T(-\mathbf{P}_0)\mathbf{x} + r_0^2 \geq 0, \\ \mathbf{P}_0 &= \begin{bmatrix} 14.09^2 & 0 \\ 0 & 11.07^2 \end{bmatrix}, \; \mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \; r_0 = 0.2.\end{aligned} \tag{26}$$

For the CSTR system (22), the following two scenarios are considered:

(i) open-loop system, that is, $u = 0$ l/s,
(ii) closed-loop system, that is, $u = -\mathbf{K}\mathbf{x}$ where $\mathbf{K} = [0.9907 \;\; 0.0954]$ was obtained by a linear quadratic regulator (LQR) design procedure considering the linearized system (22) at the nominal operating point.

We parameterize the barrier certificate polynomial of order 2 as $B(\mathbf{x}) = \sum_i b_i \mathbf{x}^{\boldsymbol{\alpha}_i}$, $\boldsymbol{\alpha}_1 = [2 \;\; 0]$, $\boldsymbol{\alpha}_2 = [0 \;\; 2]$, $\boldsymbol{\alpha}_3 = [1 \;\; 1]$, $\boldsymbol{\alpha}_4 = [1 \;\; 0]$, $\boldsymbol{\alpha}_5 = [0 \;\; 1]$, $\boldsymbol{\alpha}_6 = [0 \;\; 0]$, where m, n in $\boldsymbol{\alpha}_i = [m \;\; n]$ indicate the degrees of the variables x_1, x_2 respectively. Similarly, the other multiplier polynomials are of order 2.

4.1 Results

The resulting maximum unsafe set for the open-loop case and the closed-loop case are shown in fig. (4) in the original state space. The zero-level contour of the barrier certificate separates the initial set and the unsafe set. The solid curves represent the system trajectories for $d = 1.8708$ mol/l while the dashed curves represent the system trajectories for $d = -1.8708$ mol/l. Observe that the obtained unsafe set is almost the optimal upper bound of the maximum reachability of the system.

Table (1) shows a comparision between the numerical approaches used to solve the optimization problem. The iterative approach was initialized with $B(\mathbf{x}) = \mathbf{x}^T\mathbf{P}_0\mathbf{x} - 0.05$ in both cases while PENBMI initializes all the unknown coefficients, by default, as 0. The iterative approach as well as the penalty/augmented Lagrangian method provide a feasible solution while the theory of moments approach, though theoretically rigorous, failed to arrive at a feasible solution due to high memory requirements.

The maximum unsafe set for the open-loop case (see Fig. (4(a))) is given by

$$\begin{aligned}g_u(c_a, c_b) &= (c_a - 1.235)^2 + (c_b - 0.9)^2 - 0.29614 \geq 0 \\ &\quad \text{(iterative approach)}, \\ g_u(c_a, c_b) &= (c_a - 1.235)^2 + (c_b - 0.9)^2 - 0.2962 \geq 0 \\ &\quad \text{(penalty/augmented Lagrangian approach)}.\end{aligned}$$

The maximum unsafe set for the closed-loop case (see Fig. (4(b))) is given by

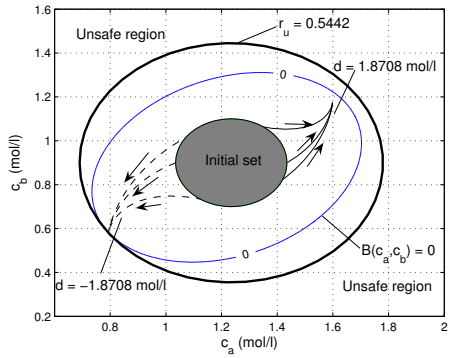
$$\begin{aligned}g_u(c_a, c_b) &= (c_a - 1.235)^2 + (c_b - 0.9)^2 - 0.046951 \geq 0 \\ &\quad \text{(iterative approach)}, \\ g_u(c_a, c_b) &= (c_a - 1.235)^2 + (c_b - 0.9)^2 - 0.0430 \geq 0 \\ &\quad \text{(penalty/augmented Lagrangian approach)}.\end{aligned}$$

5. SUMMARY AND CONCLUSIONS

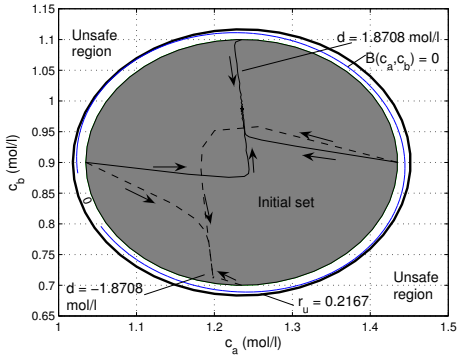
In this paper, a method to prove the safety of an uncertain non-linear polynomial system was presented using the sum-of-squares decomposition. For the CSTR system, safety was proved for the open-loop as well as the closed-loop case. The involved BMI problem was solved using

Table 1. Computational times of numerical approaches for solving the optimization problem for the 2^{nd}-order CSTR system. The iterative and penalty/aug. Lagrangian methods were solved on an Intel Celeron processor, 2.40 GHz, 512 MB RAM while the moments method was solved on an AMD Dual-Opteron processor, 2.40 GHz, 8 GB RAM.

Approach	**Solver**	**Comput. time (open-loop/closed-loop)**
Iterative	SeDuMi	at-least 1 hour for each case
Penalty/Aug. Lagrangian	PENBMI	17.5 sec. / 8.3 sec.
Theory of Moments	SOLVEMOMENT	fails due to high memory requirements



(a) Barrier certificate and unsafe set for the open-loop system.



(b) Barrier certificate and unsafe set for the closed-loop system.

Fig. 4. Barrier certificates for the 2^{nd}-order CSTR system.

three different methods. The results from the iterative approach and the penalty/augmented Lagrangian approach are almost equivalent; however, the former method is much slower compared to the latter one. The theory of moments, though theoretically rigorous, failed in practice for our problem mainly due to high memory requirements.

Due to the bilinear (non-convex) nature of the optimization problem, the available BMI solvers (SOLVEMOMENT and PENBMI) do not guarantee convergence towards a feasible solution, especially when the system order is increased. Moreover, the success of the PENBMI solver depends on an appropriate initialization of the decision variables. Therefore, the iterative approach seems to be more attractive in the case of higher system orders. However, as explained in section 3.2, the problem must be appropriately initialized which could be difficult for higher-order systems. Hence, a method to initialize the iterative approach in such cases must be investigated further.

ACKNOWLEDGEMENTS

We would like to specially thank Johan Löfberg from the Dept. of Electrical Engg., Linköping University, Sweden and Didier Henrion from LAAS-CNRS, France for their support and for the numerous discussions we had with them.

REFERENCES

S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan. *Linear Matrix Inequalities in System and Control Theory.* SIAM, Philadelphia, PA, 1994.

H. K. Khalil. *Nonlinear Systems.* Prentice-Hall, Inc., Upper Saddle River, NJ, second edition, 1996.

K. U. Klatt and S. Engell. Gain-scheduling trajectory control of a continuous stirred tank reactor. *Computers & Chem. Engg.*, 22(4-5):491–502, 1998.

J. B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization*, 11(3):796–817, 2001.

Johan Löfberg. YALMIP: a toolbox for modelling and optimization in MATLAB. *IEEE Intl. Symp. on Computer Aided Control Systems Design*, pages 284–289, Sept. 2004. http://control.ee.ethz.ch/∼joloef/yalmip.php.

Y. Nesterov and A. Nemirovsky. *Interior-Point Polynomial Algorithms in Convex Programming.* SIAM, Philadelphia, USA, 1994.

A. Papachristodoulou and S. Prajna. On the Construction of Lyapunov Functions Using the Sum of Squares Decomposition. In *Proc. of the 41st IEEE CDC*, volume 3, pages 3482 – 3487, 2002.

A. Papachristodoulou and S. Prajna. *Lecture Notes in Control and Information Sciences: Positive Polynomials in Control*, volume 312, chapter Analysis of Non-polynomial Systems Using the Sum of Squares Decomposition. Springer-Verlag, Berlin/Heidelberg, 2005.

P. A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry methods in Robustness and Optimization.* PhD thesis, CalTech, Pasadena, CA, 2000.

S. Prajna and A. Jadbabaie. *Hybrid Systems: Computation and Control*, chapter Safety Verification of Hybrid Systems Using Barrier Certificates, pages 477–492. Springer-Verlag, 2004.

M.A. Savageau and E. O. Voit. Recasting Nonlinear Differential-Equations as S-Systems - A Canonical Nonlinear Form. *Math. Biosciences*, 87:83–115, 1987.

G. Stengle. A Nullstellensatz and a Positivstellensatz in semialgebraic geometry. *Mathematische Annalen*, 207: 87–97, 1974.

M. Stingl. *On the Solution of Nonlinear Semidefinite Programs by Augmented Lagrangian Methods.* PhD thesis, Universität Erlangen-Nürnberg, Germany, 2005.

J. F. Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization Methods and Software*, 11(1-4):625–653, 1999. http://sedumi.mcmaster.ca/.