Proceedings of the 45th IEEE Conference on Decision & Control
Manchester Grand Hyatt Hotel
San Diego, CA, USA, December 13-15, 2006

Degree Bounds for Polynomial Verification of the Matrix Cube Problem

Been-Der Chen[1,3] Sanjay Lall[2,3]

Abstract

In this paper we consider the problem of how to computationally test whether a matrix inequality is positive semidefinite on a semi-algebraic set. We propose a family of sufficient conditions using the theory of matrix Positivstellensatz refutations. When the semi-algebraic set is a hypercube, we give bounds on the degree of the required certificate polynomials.

1 Introduction

In this paper we consider the following problem.

Problem 1. *Suppose $H_0, \dots, H_m \in \mathbb{R}^{n\times n}$ are symmetric matrices, and $\Delta \subset \mathbb{R}^m$. Define the affine map $G : \mathbb{R}^m \to \mathbb{R}^{n\times n}$ by*

$$G(\delta) = H_0 + \sum_{i=1}^{m} \delta_i H_i$$

for all $\delta \in \mathbb{R}^m$. We would like to know if

$$G(\delta) \geq 0 \text{ for all } \delta \in \Delta.$$

This problem is a *robust semidefinite program*, and it has many important applications in control and optimization. One motivating application is testing *quadratic stability*, as follows. Consider the parameterized family of linear time-invariant systems

$$\dot{x} = \Big(A_0 + \sum_{i=1}^{m} \delta_i A_i\Big)x$$

Here $\delta \in \mathbb{R}^m$ is a vector of *uncertain parameters*. We would like to check whether the above system is stable for all $\delta \in \Delta$. This problem has been addressed in [16, 23, 19]. A well-known approach is to seek a quadratic Lyapunov function which proves stability for all parameters within the uncertainty set Δ. That is, we would like to find a positive definite matrix $P \in \mathbb{R}^{n\times n}$ such that

$$\Big(A_0 + \sum_{i=1}^{m} \delta_i A_i\Big)^T P + P\Big(A_0 + \sum_{i=1}^{m} \delta_i A_i\Big) < 0$$

for all $\delta \in \Delta$. Testing whether P satisfies this inequality is equivalent to Problem 1, via the identification $H_i = -A_i^T P - PA_i$ for $i = 0, \dots, m$.

More generally, we can convert a wider class of robust optimization problems to the form of Problem 1. We would like to solve

$$\begin{aligned} \min \quad & c^T x \\ \text{subject to} \quad & \mathcal{A}^0 + \sum_{i=1}^{m} x_i \mathcal{A}^i \geq 0 \\ & \qquad \text{for all } (\mathcal{A}^0, \dots, \mathcal{A}^n) \in \mathcal{U} \end{aligned}$$

where the set of matrix tuples $\mathcal{U}$ is given by

$$\mathcal{U} = \left\{ \begin{array}{l} (A_1, \dots, A_n) = \\ \quad (A_0^0, \dots, A_n^0) + \displaystyle\sum_{k=1}^{m} \delta_i (A_0^k, \dots, A_n^m) \end{array} \middle| \; \delta \in \Delta \right\}$$

To find the optimal solution to this robust semidefinite problem, we need to be able to efficiently verify that a given x satisfies the constraints, and this is equivalent to Problem 1.

Problem 1 has been addressed in the literature. Although Problem 1 has many important applications, the verification is hard for most uncertainty sets. When the uncertainty set is an ellipsoid, the problem may be converted to a binary optimization problem [3]. When the uncertainty set is a hypercube, Problem 1 is called the *matrix cube problem*, and it was shown to be NP hard in [14]. In the case when the uncertainty set is a bounded polytope, it is sufficient to check the matrix inequality at the vertices. Notice that in the case when Δ is a cube there are 2^m vertices, and so this approach scales very poorly as m grows. Similar results are shown for the quadratic stability problem [2, 6].

To reduce computational complexity , several sufficient conditions have been proposed, such as the use of the $\mathcal{S}$-procedure to construct a set of scalar certificates [7]. Ben-Tal and Nemirovski also proposed a stronger condition which does not exhibit the above poor scaling [4]. In this paper we will generalize this condition, so we state it here. Here $\mathbb{S}^n$ denotes the set of real $n \times n$ symmetric matrices.

Theorem 2. *Suppose Δ is the cube*

$$\Delta = \big\{\, \delta \in \mathbb{R}^m \mid |\delta_i| \leq 1 \text{ for all } i \,\big\}$$

[1]Email: bdchen@stanford.edu
[2]Email: lall@stanford.edu
[3]Department of Aeronautics and Astronautics, Stanford University, Stanford CA 94305-4035, U.S.A.
Both authors were partially supported by the Stanford MICA *Coordination and Control for Networks of Interacting Automata*, DARPA/SPAWAR award number N66001-01-C-8080

Define the set $\mathcal{X}_T \subset \mathbb{S}^n \times \cdots \times \mathbb{S}^n$, where $(X_1, \ldots, X_m) \in \mathcal{X}_T$ if and only if

$$\begin{aligned} H_0 - \sum_{i=1}^{m} X_i &\geq 0, \\ X_i + H_i &\geq 0, \qquad \text{for all } i = 1, \ldots, m \\ X_i - H_i &\geq 0, \qquad \text{for all } i = 1, \ldots, m. \end{aligned}$$

Then $G(\delta)$ is positive semidefinite for all $\delta \in \Delta$ if $\mathcal{X}_T$ is not empty.

This condition may be tested via semidefinite programming. The paper [4] also shows that if the above SDP condition is infeasible then there exists a δ within a larger cube such that $G(\delta)$ is not positive semidefinite. This gives an estimate of the conservativeness of this test.

The matrix cube problem (and also therefore Problem 1) is closely related to binary quadratic programming. Here, we would like to find

$$\begin{array}{ll} \min & x^T A x \\ \text{subject to} & x \in \{-1, 1\}^n \end{array}$$

Without loss of generality we may assume A is positive definite, and it is then straightforward to see that the problem is equivalent to the following matrix cube problem.

$$\begin{array}{ll} \max & t \\ \text{subject to} & \begin{bmatrix} t & x^T \\ x & A^{-1} \end{bmatrix} \geq 0 \quad \text{for all } x \in \{-1, 1\}^n \end{array}$$

In general such quadratic programs are hard, and much research has been done to address this, for example, using the Lagrangian relaxation to compute a lower bound on the optimal value [21], or using semidefinite programming via a lifting approach [13], or using semidefinite program to find the lower bound of the MAXCUT problem [8]. The gap between the relaxed problem and the actual problem may be reduced by introducing additional variables and redundant constraints [1]. Lasserre used an approach based on moments and showed that one needs at most $2^m - 1$ additional variables [11, 12] for an exact solution. This approach is also related to the dual of the refutation approach adopted in this paper.

In this paper, instead of searching a set of scalar certificates using the $\mathcal{S}$-procedure, we will construct a sufficient condition via a search for a polynomial certificates. If such a certificate exists, then there is no $\delta \in \Delta$ such that the affine function G is not positive semidefinite. Our approach is applicable to general semi-algebraic uncertainty sets, including ellipsoids and hypercubes. In this formulation, we construct a family of refutation sets which have a hierarchical structure. If the current refutation set does not yield a feasible certificate, we may seek for higher degree certificates. Similar approaches have been used to analyze and synthesize output feedback controllers for LPV systems [22].

For some uncertainty sets we will also show that if there is no $\delta \in \Delta$ for which G is not positive semidefinite, then there will exists a certificate of specific degree. When the uncertainty set is a hypercube, we show that the highest degree needed is at most $2m$. We also study the case when the certificates are restricted to be quadratic and we show the resulting condition is tighter than the best existing result of Theorem 2. In addition, we give several cases when our conditions using quadratic certificates are necessary and sufficient. Finally, we give some numerical examples to compare our results with others.

2 Preliminaries

We use the following standard notation. The matrix I_n is the $n \times n$ identity. For $X \in \mathbb{S}^n$, the notation $X \geq 0$ means that X is positive semidefinite. The vector $e_i \in \mathbb{R}^n$ has the ith entry equal to 1 and all other entries equal to zero. The vector $\mathbf{1} \in \mathbb{R}^n$ has all entries equal to 1.

The set $\mathbb{R}[x_1, \ldots, x_n]$ is the ring of polynomials in n variables with real coefficients. We often abbreviate $\mathbb{R}[x_1, \ldots, x_n]$ to simply $\mathbb{R}[x]$. Every polynomial $f \in \mathbb{R}[x]$ can be written as

$$f = \sum_{\alpha \in W} c_\alpha x^\alpha$$

where $W \subset \mathbb{N}^n$, and the notation x^α is defined by

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

A polynomial $g \in \mathbb{R}[x]$ is a *sum of squares (SOS)* if it can be expressed as

$$g(x) = \sum_{i=1}^{n} f_i(x)^2$$

for some polynomials $f_i \in \mathbb{R}[x]$. We use $\Sigma[x]$ to represent the set of sum-of-squares polynomials in $\mathbb{R}[x]$, and abbreviate it to Σ when the dimension is clear from the context. We also extend this definition matrix polynomials as follows.. Let $\mathbb{R}[x]^{m \times n}$ denote the set of $m \times n$ polynomial matrices and $\mathbb{S}[x]^n$ denote the set of $n \times n$ symmetric polynomial matrices. We define the notion of *sum-of-squares* for matrix polynomials as follows

Definition 3. *A matrix polynomial $S \in \mathbb{S}[x]^m$ is called a sum-of-squares if there exist polynomial vectors $T_1, \ldots, T_r \in \mathbb{R}[x]^m$ such that*

$$S(x) = \sum_{i=1}^{r} T_i(x) T_i(x)^T.$$

This is a generalization of SOS representation used for scalars. We will use $\Sigma[x]^n$ to represent the set of $n \times n$ SOS polynomial matrices. We also define two specific sets $\mathcal{Q}_1$, $\mathcal{Q}_2$ which will be useful in later sections.

Definition 4. *Let $W_1 = \{\alpha \in \mathbb{N}^m \mid \alpha_i \le 2$ for all $i = 1, \dots, m\}$ and $W_2 = \{\alpha \in \mathbb{N}^m \mid \sum_{i=1}^m \alpha_i \le 2\}$. The sets $\mathcal{Q}_1$, $\mathcal{Q}_2$ are defined as*

$$\mathcal{Q}_1 = \Big\{ \sum_{\alpha \in W_1} C_\alpha \delta^\alpha \mid C_\alpha \in \mathbb{S}^n \text{ for all } \alpha \in W_1 \Big\}$$
$$\mathcal{Q}_2 = \Big\{ \sum_{\alpha \in W_2} C_\alpha \delta^\alpha \mid C_\alpha \in \mathbb{S}^n \text{ for all } \alpha \in W_2 \Big\}$$

Note that polynomials in $\mathcal{Q}_1$ have degree less than or equal to $2m$ and polynomials in $\mathcal{Q}_2$ have degree less than or equal to 2.

When $F \in \Sigma[x]^n$, it is clear that $F(x)$ is positive semidefinite for all $x \in \mathbb{R}^n$. One may address positive semidefiniteness of a matrix polynomial over a restricted domain using the following lemma, which gives a sufficient condition.

Lemma 5. *Suppose $f_1, \dots, f_n \in \mathbb{R}[x]$ and $Q \in \mathbb{R}[x]^m$ is a symmetric matrix polynomial. Define the set*

$$\mathcal{D} = \Big\{ x \in \mathbb{R}^n \mid f_i(x) \ge 0 \text{ for all } i = 1, \dots, m \Big\}$$

Then, $Q(x) \ge 0$ for all $x \in \mathcal{D}$ if there exist SOS polynomial matrices $S_0, S_1, \dots, S_n \in \Sigma[x]^m$ such that

$$Q(x) = S_0(x) + \sum_{i=1}^n S_i(x) f_i(x)$$

It is also known that if $\mathcal{D}$ is compact, and with additional technical restrictions, then the above condition is also necessary [20]; this is an extension of a well-known result by Putinar [17].

3 Positivstellensatz refutations

In this section, we will study Problem 1 when the set Δ is semi-algebraic, that is

$$\Delta = \Big\{ \delta \in \mathbb{R}^m \mid f_i(\delta) \ge 0, \text{ for } i = 1, \dots, m \Big\}$$

where $f_1, \dots, f_m \in \mathbb{R}[\delta]$. It is clear that a cube and an ellipsoid can be expressed as semi-algebraic sets. The following condition provides a simple condition under which $G(\delta)$ is positive semidefinite for all $\delta \in \Delta$.

Theorem 6. *The matrix polynomial $G(\delta)$ is positive semidefinite for all $\delta \in \Delta$ if there exist SOS polynomial matrices $S_0, S_1, \dots, S_m$ satisfying*

$$G(\delta) = S_0 + \sum_{i=1}^m S_i f_i(\delta) \tag{1}$$

This is a simple consequence of Lemma 5 and we may view it as provided a certificate refuting the existence of $\delta \in \Delta$ such that $G(\delta)$ is not within the positive semidefinite cone. The certificate is the sequence of polynomials $S_0, \dots, S_m$. As discussed in the previous section, this condition is also necessary if additional technical conditions on Δ are satisfied [20] (both polytopes and ellipsoids satisfy these conditions.)

One thing we have not yet specified is the degree of the certificates required. Although we may pursue high degree certificates, the computational complexity of finding $S_0, \dots, S_m$ grows rapidly as we search over sets containing high-degree polynomials. In many applications of this refutation approach, a bound on the degree of the required certificates is not known. However, in some cases, we can show a degree bound. In this paper, we focus on the matrix cube problem, i.e., hypercube uncertainty set, and we will show the degree is bounded. As mentioned earlier, the hypercube uncertainty set satisfies the technical condition, also the vertices of the cube. This implies the refutation provides a necessary and sufficient condition to verify the matrix cube problem.

Theorem 7. *Define the set $\mathcal{X}_1 \subset \Sigma[\delta]^n \times \mathbb{S}[\delta]^n \times \dots \times \mathbb{S}[\delta]^n$ such that $(S_0, S_1, \dots, S_m) \in \mathcal{X}_1$ if and only if*

$$G(\delta) = S_0 + \sum_{i=1}^m (1 - \delta_i^2) S_i. \tag{2}$$

Then, $G(\delta) \ge 0$ for all δ within the unit cube if and only if $\mathcal{X}_1$ is not empty.

The above theorem shows that $S_1, \dots, S_m$ only need to be symmetric matrix polynomials instead of SOS matrix polynomials. We further show the highest degree of certificate required is $2m$.

Theorem 8. *Define the set $\mathcal{X}_2 \subset \mathcal{X}_1$ such that $(S_0, \dots, S_m) \in \mathcal{X}_2$ if and only if $(S_0, \dots, S_m) \in \mathcal{X}_1$ and $S_1, \dots, S_m \in \mathcal{Q}_1$. Then, $G(\delta) \ge 0$ for all δ within the unit cube if and only if $\mathcal{X}_2$ is non-empty.*

Before proving the theorem, we show two lemmas.

Lemma 9. *Suppose there are two symmetric matrices $A, B \in \mathbb{S}^n$ satisfying $-A \le B$ and $B \le A$. Then*

$$\begin{bmatrix} A & B \\ B & A \end{bmatrix} \ge 0.$$

This lemma convert two linear matrix inequalities into one bigger LMI. We may use the above lemma to eliminate δ into a semidefinite program with one large linear matrix inequality. The following lemma states this result and shows the structure of this LMI.

Lemma 10. *Suppose $H_0, \dots, H_m \in \mathbb{S}^n$. Define the block diagonal matrices*

$$G_k = \begin{bmatrix} H_k & & \\ & \ddots & \\ & & H_k \end{bmatrix} \in \mathbb{S}^{2^{k-1}n}, \quad \text{for } k = 1, \dots, m.$$

and recursively define the sequence $N_0, N_1, \dots, N_m$ by

$$N_k = \begin{bmatrix} N_{k-1} & G_k \\ G_k & N_{k-1} \end{bmatrix} \qquad N_0 = H_0$$

Then $N_m \geq 0$ if and only if

$$H_0 + \sum_{i=1}^{m} \delta_i H_i \geq 0, \qquad \text{for all } \delta \in \{-1,1\}^m. \tag{3}$$

This result gives an equivalent condition to test the matrix cube problem. We now prove Theorem 8 using the above lemmas.

Proof of Theorem 8. Sufficiency is implied by Theorem 6 and we will now prove necessity. Suppose $G(\delta) \geq 0$ for all δ within the unit cube. Lemma 10 shows that $N_m \geq 0$. Let $z_0 = 1$ and recursively define a sequence of vectors of monomials $z_0, z_1, \dots, z_m$ as follows

$$z_i = \begin{bmatrix} z_{i-1} \\ \delta_i z_{i-1} \end{bmatrix} \qquad \text{for } i = 1, \dots, m.$$

We choose $S_0 = 2^{-m}(z_m \otimes I)^T N_m (z_m \otimes I)$ and it is clear that $S_0 \in \Sigma[x,\delta] \cap \mathcal{Q}_1$. As for $S_1, \dots, S_m$, we let $\mathcal{D} = \{1, \dots, m\}$ and define the sets $\mathcal{E}_{k,l}, \mathcal{F}_{j,k,l}$ as follows,

$$\mathcal{E}_{k,l} = \Big\{ A \subset \mathcal{D} \mid |A| = l \text{ and } k \notin A \Big\},$$
$$\mathcal{F}_{j,k,l} = \Big\{ A \subset \mathcal{D} \mid |A| = l, \text{ and } j,k \notin A \Big\}.$$

We also define the polynomials

$$p_{k,l} = \sum_{A \in \mathcal{E}_{k,l}} \prod_{j \in A} \delta_j^2, \qquad q_{j,k,l} = \sum_{A \in \mathcal{F}_{j,k,l}} \prod_{p \in A} \delta_p^2$$

Let $S_1, \dots, S_m$ as follows

$$\begin{aligned} S_k = H_0 &\left(c_1 + \sum_{i=1}^{m-1} c_{i+1} p_{k,i} \right) \\ &+ \sum_{\substack{i=1 \\ i \neq k}}^{m} \delta_i H_i \left(d_1 + \sum_{j=1}^{m-2} d_{j+1} q_{i,k,j} \right) \\ &\qquad \text{for } k = 1, \dots, m \end{aligned}$$

where $c \in \mathbb{R}^m$ and $d \in \mathbb{R}^{m-1}$ satisfy

$$M(m)c = e_1 - 2^{-m}\mathbf{1}, \quad M(m-1)d = e_1 - 2^{-m+1}\mathbf{1}$$

and $M : \mathbb{R} \mapsto \mathbb{R}^{m \times m}$ are

$$M(m) = \begin{bmatrix} m & 0 & \cdots & 0 \\ -1 & m-1 & \ddots & \vdots \\ & \ddots & \ddots & 0 \\ 0 & \cdots & -m+1 & 1 \end{bmatrix}.$$

The highest degree of $S_1, \dots, S_m$ in each δ_i is at most 2 which implies that $S_1 \dots, S_m \in \mathcal{Q}_1$. Expanding $S_0 + \sum_{i=1}^{m}(1-\delta_i^2)S_i$ shows that $S_0, \dots, S_m$ satisfy (2). □

The reason that degree bounded $S_0, S_1, \dots, S_m$ exist is because of the persymmetric structure of N_m. We now have a family of refutations for the matrix cube problem and we may check if $G(\delta) \geq 0$ for all $\delta \in \Delta$ by searching a certificate of degree at most $2m$.

This condition may also be directly expressed as a semidefinite program. Although the degree bound on the certificates grows linearly with m, the number of monomials required to express the certificates (i.e., the dimension of $\mathcal{Q}_1$) grows exponentially in m. Of course, since we have exactly solved the problem this is expected; the original problem is NP-hard.

When the cube is high-dimensional, the computational complexity of searching $\mathcal{X}_2$ also scales poorly. To reduce computational effort, we may limit the search to low degree certificates and we turn our focus to the search of the quadratic set $\mathcal{X}_3$ as follows.

Definition 11. *Define the set $\mathcal{X}_3 \subset \mathcal{X}_2$ such that $(S_0, \dots, S_m) \in \mathcal{X}_3$ if and only if $(S_0, \dots, S_m) \in \mathcal{X}_2$ and $S_0 \in \mathcal{Q}_2$, $S_1, \dots, S_m \in \mathbb{S}^n$.*

The computational complexity of searching $\mathcal{X}_3$ is lower. The equivalent semidefinite program for testing the nonemptiness $\mathcal{X}_3$ as follows

$$\begin{aligned} \text{find} \quad & X_1, \dots, X_m \in \mathbb{S}^n, L \in \mathbb{S}^{n(m+1)} \\ \text{s.t.} \quad & L = \begin{bmatrix} L_{00} & \cdots & L_{0m} \\ \vdots & \ddots & \vdots \\ L_{0m}^T & \cdots & L_{mm} \end{bmatrix} \geq 0 \\ & 0 = \sum_{i=0}^{m} L_{ii} - H_0 \\ & 0 = L_{ii} - X_i \qquad \text{for } i = 1, \dots, m \\ & 0 = L_{0i} + L_{0i}^T - H_i \qquad \text{for } i = 1, \dots, m \\ & 0 = L_{ij} + L_{ij}^T \qquad \text{for } i,j = 1, \dots, m, i \neq j \end{aligned} \tag{4}$$

If the above semidefinite program is feasible, we may construct the certificate by choosing $S_i = X_i$ for $i = 1, \dots, m$ respectively and $S_0 = z^T L z$ where $z = \begin{bmatrix} 1 \\ \delta \end{bmatrix} \otimes I$.

The gap between verifying the matrix cube problem and checking the non-emptiness of $\mathcal{X}_3$ can be interpreted as the degree difference between certificates in $\mathcal{X}_2$ and $\mathcal{X}_3$. The degree of certificates in $\mathcal{X}_3$ is at most 2, instead of growing linearly with respect to m. Although this means that the condition is conservative, we now show that it is still tighter than the previously well-known condition in Theorem 2.

Theorem 12. *If $\mathcal{X}_T$ is not empty, then $\mathcal{X}_3$ is not empty.*

Proof. Suppose $(X_1, \dots, X_m) \in \mathcal{X}_T$. It is clear that X_i is positive definite for $i = 1, \dots, m$. From Lemma 9, $X_1, \dots, X_m$ also satisfy

$$\begin{bmatrix} X_i & H_i \\ H_i & X_i \end{bmatrix} \geq 0, \qquad \text{for } i = 1, \dots, m$$

which by the Schur complement implies

$$X_i \geq H_i X_i^{-1} H_i, \qquad \text{for } i = 1, \dots, m.$$

Thus,

$$H_0 - \frac{1}{2}\sum_{i=1}^{m} X_i - \frac{1}{2}\sum_{i=1}^{m} H_i X^{-1} H_i \geq H_0 - \sum_{i=1}^{m} X_i \geq 0.$$

Applying the Schur complement again gives

$$J = \begin{bmatrix} H_0 - \frac{1}{2}\sum_{i=1}^{m} X_i & \frac{1}{2}H_1 & \cdots & \frac{1}{2}H_m \\ \frac{1}{2}H_1 & \frac{1}{2}X_1 & & 0 \\ \vdots & & \ddots & \\ \frac{1}{2}H_m & 0 & & \frac{1}{2}X_m \end{bmatrix} \geq 0 \quad (5)$$

By letting

$$S_0 = \begin{bmatrix} I \\ \delta \otimes I \end{bmatrix}^T J \begin{bmatrix} I \\ \delta \otimes I \end{bmatrix},$$
$$S_i = \frac{1}{2}X_i, \quad \text{for } i = 1, \ldots, m.$$

we show $(S_1, \ldots, S_m)$ satisfies (2) and this completes the proof. □

The above theorem shows that every certificate in $\mathcal{X}_T$ has a corresponding instance in $\mathcal{X}_T$. We show that our condition is strictly tighter than the previous condition via a counterexample in Section 4. Comparing the two semidefinite programs, we recognize that (5) imposes constraints on the off-diagonal entries such that $L_{ij} = 0$ for $i, j = 1, \ldots, m, i \neq j$. The entries are relaxed to be skew symmetric in (4) and this condition is still sufficient.. This skew symmetric structure arises naturally in the Positivstellensatz refutation.

To see the relationship of the conditions so far, we show the relationship between the refutation sets in Figure 1. The set $\mathcal{X}_1$ and $\mathcal{X}_2$ are the two largest refutation sets and the computational complexity of searching these sets grows exponentially with respect to the dimension of the cube. If we limit the search in the set $\mathcal{X}_3$, then computational complexity is reduced and the result is still tighter than the existing conditions $\mathcal{X}_T$.

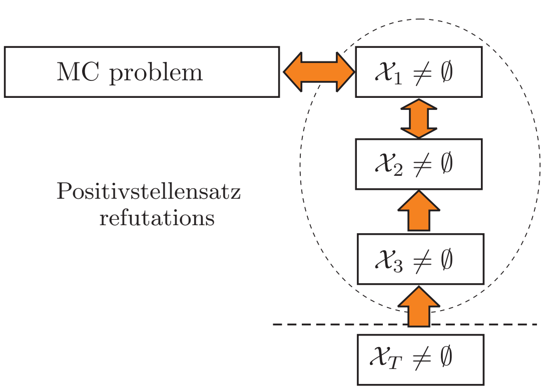

Figure 1: Set hierarchy

Note that although searching for quadratic certificates is only a sufficient condition for the matrix cube problem, the condition sometimes is also necessary, for example, when the the number of uncertainty parameters m is less than or equal to 2.

Theorem 13. *Suppose $m \leq 2$. Then $G(\delta) \geq 0$ for all δ within the unit cube if and only if there exists $(S_0, S_1, S_2) \in \mathcal{X}_3$.*

For the case when $m > 2$, it is unknown whether a similar equivalence holds. However, if $H_1, \ldots, H_m$ are either positive or negative semidefinite, quadratic certificates again provide necessary conditions.

Theorem 14. *Suppose the matrices $H_1, \ldots, H_m$ are either positive semidefinite or negative semidefinite, then $G(\delta) \geq 0$ for all δ within the unit cube if and only if there exist $(S_0, S_1, \ldots, S_m) \in \mathcal{X}_3$.*

The proofs are omitted due to space constraints. The above theorems allow us to limit the search to quadratic certificates in many cases. We now give an example to show the tightness of the refutation condition.

4 Examples : Quadratic stability

In this section, we check quadratic stability of a linear time-invariant system to provide a specific numerical example. Consider the uncertain system

$$\dot{x} = (A_0 + \sum_{i=1}^{m} \delta_i A_i)x$$

where $\|\delta\|_\infty \leq R$. We would like to compute the largest R such that the system is quadratically stable for all δ within the cube.

First, we study the case when there are only two uncertainty variables as follows.

$$\dot{x}(t) = \begin{bmatrix} -0.4 & 0 & -0.3\delta_1 + 1 \\ 0 & -3.2 & 0.3\delta_1 - 0.5 \\ 0.4\delta_2 - 0.8 & 0.3\delta_2 - 2.2 & \delta_1 - 1.7 \end{bmatrix} x(t).$$

We compute the largest such R for which all δ within the corresponding cube lead to stability. We similarly compute the largest cube admitting quadratic stability, and the bounds on this cube obtained using quadratic certificates and Theorem 2 from Ben-Tal and Nemirovski. These are shown in Figure 2. As discussed in the previous section, the bound obtained using quadratic certificates is exact, and we do not need to pursue higher degree certificates.

5 Conclusions

The question of degree bounds for positivstellensatz refutations is one of significant importance for practical use of semidefinite programming for matrix polynomial optimization. In this paper, we showed that

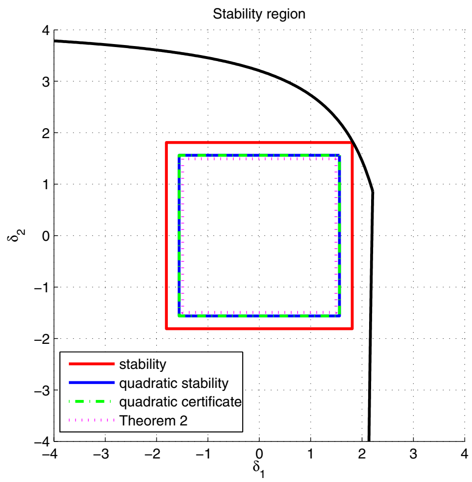

Figure 2: stability bound from various conditions

meaningful bounds can be obtained. We used matrix Positivstellensatz refutations to test positive semidefiniteness of an affine function over a given uncertainty set. When the uncertainty set is a hypercube, we show that the highest degree certificate needed is $2m$. Although the certificates are degree bounded, computational complexity is still high in general. To reduce the complexity, we study the case of quadratic certificates and show that the bounds obtained are still tighter than those obtained from existing conditions. We also show several cases when refutation using quadratic certificates is exact. This result may be useful in analyzing and synthesizing a robust controller for systems with uncertainties and robust quadratic optimization.

References

[1] K. Anstreicher and H. Wolkowicz. On Lagrangian relaxation of quadratic matrix constraints. *Siam J. matrix anal.*, 22:41–55, 2000.

[2] H. P. Horisberger; P. R. Belanger. Regulators for linear, time invariant plants with uncertain parameters. *IEEE Transactions on Automatic Control*, 21(5):705–708, 1976.

[3] A. Ben-Tal and A. Nemirovski. Robust convex optimization. *Mathematics of operational reserch*, 23:769–805, 1998.

[4] A. Ben-Tal and A. Nemirovski. On tractable approximations of uncertain linear matrix inequalities affected by interval uncertainty. *SIAM Journal On Optimization*, 12(3):811–833, 2002.

[5] S. Boyd and Q. Yang. Structured and simultaneous Lyapunov functions for system stability problems. *International Journal of Control*, 49:2215–2240, 1989.

[6] S. Boyd and Q. Young. Structured and simultaneous Lyapunov functions for system stability problems. *Int. J. Control*, 49:2215–2240, 1989.

[7] S. Boyd; L. E. Ghaoui; E. Feron. *Linear Matrix Inequalities in System and Control Theory.* SIAM, 1994.

[8] M. Goemans and D. Williamson. Improved approximation algorithm for maximum cut. and satisfiability problems using semidefinite programming. *J. Assoc. Comput. Mach*, 42:1115–1142, 1995.

[9] M. X. Goemans. Semidefinite programming in combinatorial optimization. *Math. Programming*, 79:143–162, 1997.

[10] P.P. Khargonekar, I.R. Petersen, and K. Zhou. Robust stabilization of uncertain linear systems: quadratic stabilizability and H^∞ control theory. *IEEE Transactions on Automatic Control*, 35(3):356–361, 1990.

[11] Jean B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. optim.*, 11:796–817, 2001.

[12] Jean B. Lasserre. Global optimization with polynomials and the problem of moments. *Lecture Notes in Computer Science*, 2081:293–303, 2001.

[13] L. Lovász and A. Schrijver. Cones of matrices and set-functions and 0-1 optimization. *SIAM J. Optim.*, 1:166–190, 1991.

[14] A. Nemirovski. Several NP-hard problems arising in robust stability analysis. *Math. Control Signals Systems*, 6:99–105, 1993.

[15] I. R. Petersen. Notions of stabilizability and controllability for a class of uncertain linear systems. *Int. J. Control*, 46:409–422, 1987.

[16] V. Popov. Nouveaux criterium de stabilite pour les systems automatiques nonlineares. *Revue d'Electrotechnique et d'Energetique*, 5(1):72–88, 1960.

[17] M. Putinar. Positive polynomial on compact semialgebraic sets. *Indiana Unversity Mathematics Journal*, 42:969–984, 1993.

[18] M.A. Rotea, M. Corless, D. Da, and I.R. Petersen. Systems with structured uncertainty: relations between quadratic and robust stability. *IEEE Transactions on Automatic Control*, 38(5):799–803, 1993.

[19] M.G. Safonov. Optimal diagonal scaling for infinity-norm optimization. *Syst. Control Letters*, 7:257–260, 1986.

[20] C. Scherer and C. Hol. Asymptotically exact relaxations for robust lmi problems based on matrix-valued sum-of-squares. In *Proceedings of the 16th Mathematical Theory of Networks and Systems Conference*, 2004.

[21] N.Z. Shor. Quadratic optimization problems. *Tekhnicheskaya Kibernetika*, 222:128–139, 1987.

[22] F. Wu and S. Prajna. A new solution approach to polynomial lpv system analysis and synthesis. In *Proc. American Control Conference*, volume 2, pages 1362–1367, 2004.

[23] P.M. Young. Structured singular value approach for systems with parametric uncertainty. *Int. J. Robust Nonlinear Control*, 11:653–680, 2001.