HAL
open science

SPECTRA -a Maple library for solving linear matrix inequalities in exact arithmetic

Didier Henrion, Simone Naldi, Mohab Safey El Din

To cite this version:

Didier Henrion, Simone Naldi, Mohab Safey El Din. SPECTRA -a Maple library for solving linear matrix inequalities in exact arithmetic. 2016. hal-01393022v1

HAL Id: hal-01393022

https://laas.hal.science/hal-01393022v1

Preprint submitted on 5 Nov 2016 (v1), last revised 10 Feb 2020 (v3)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

SPECTRA - a Maple library for solving linear matrix inequalities in exact arithmetic

Didier Henrion* Simone Naldi† Mohab Safey El Din‡

Version 1.0 of November 5, 2016

Abstract

This document briefly describes our freely distributed Maple library SPECTRA, for Semidefinite Programming solved Exactly with Computational Tools of Real Algebra. It solves linear matrix inequalities in exact arithmetic and it is targeted to small-size, possibly degenerate problems for which symbolic infeasibility or feasibility certificates are required.

Keywords

Computer algebra, linear matrix inequalities, semidefinite programming, low rank matrices, nonnegativity certificates, sums of squares.

*LAAS-CNRS, Université de Toulouse, CNRS, Toulouse, France; Faculty of Electrical Engineering, Czech Technical University in Prague, Czech Republic.

†Technische Universität Dortmund, Fakultät für Mathematik, Dortmund, Germany.

‡Sorbonne Universités, UPMC Univ Paris 06, CNRS, INRIA Paris Center, LIP6, Equipe PolSys, F-75005, Paris, France.

1 Introduction

Given symmetric matrices $A_0, A_1, \ldots, A_n$ of size m with rational coefficients, let

$$\mathscr{S} := \{x \in \mathbb{R}^n : A(x) := A_0 + A_1 x_1 + \cdots + A_n x_n \succeq 0\}$$

denote the corresponding convex spectrahedron, defined by the linear matrix inequality (LMI) enforcing that A is positive semidefinite.

SPECTRA aims at either proving that $\mathscr{S}$ is empty, or finding at least one point in $\mathscr{S}$, using exact arithmetic.

SPECTRA should be used when the number n of variables or the size m of the LMI are small. It should not be considered as a competitor to numerical algorithms such as interior-point methods for semidefinite programming (SDP).

Contrary to numerical algorithms which are based on approximate computations and floating point arithmetic, SPECTRA is exclusively based on computations with exact arithmetic, and hence it should be primarily used either in potentially degenerate situations, for example when it is expected that $\mathscr{S}$ has empty interior, or when a rigorous certificate of infeasibility or feasibility is required. A prominent application that motivated the development of SPECTRA is the computation of certificates of positivity of real multivariate polynomials in the form of exact sum-of-squares (SOS) representations.

SPECTRA is guaranteed to compute a point x minimizing the rank of A in $\mathscr{S}$. It solves exactly the (non-convex) optimization problem

$$\begin{array}{ll} \min & \operatorname{rank} A(x) \\ \text{s.t.} & x \in \mathscr{S}. \end{array}$$

This is in sharp contrast with interior-point methods which are designed to compute a point of maximal rank.

SPECTRA is based on the theory described in [3, 4], to which the reader interested in the mathematical foundations is referred. The present document is only a brief description of the software and its main features, illustrated with small examples.

2 Getting started

SPECTRA is freely available as a library for Maple version 16 and above. It can be downloaded in the form of a single binary file `SPECTRA.mla` from the following page

`homepages.laas.fr/henrion/software/spectra`

SPECTRA relies on FGB, a library for fast computation of Gröbner bases, whose Maple interface must be installed, see [2]. SPECTRA does not work without FGB.

In a Maple worksheet, from the directory containing the file `SPECTRA.mla`, please type the command

```
> with(SPECTRA);
   [SolveLMI]
```

to activate the main function `SolveLMI`.

3 Examples

In this section we illustrate the features of SPECTRA with simple examples. Please refer to the end of this document for a more detailed description of the input and output arguments.

3.1 Half disk

Let

$$A(x) = \begin{bmatrix} 1+x_1 & x_2 & 0 \\ x_2 & 1-x_1 & 0 \\ 0 & 0 & x_1 \end{bmatrix}$$

with $n = 2$ and $m = 3$. The corresponding spectrahedron

$$\mathscr{S} = \{x \in \mathbb{R}^2 : A(x) \succeq 0\} = \{x \in \mathbb{R}^2 : 1 - x_1^2 - x_2^2 \geq 0,\ x_1 \geq 0\}$$

is a half disk. To find a point in $\mathscr{S}$, we use SPECTRA as follows:

```
> A := Matrix([[1+x1, x2, 0], [x2, 1-x1, 0], [0, 0, x1]]):
> SolveLMI(A);
  [[x1 = [0, 0], x2 = [1, 1]]]
```

This returns the point

$$x = [0, 1] \in \mathscr{S}$$

in interval arithmetic notation, i.e.

$$x_1 \in [0, 0],\ x_2 \in [1, 1]$$

and for each component in x we obtain rational (exact) lower and upper bounds. Here the bounds coincide as the point has rational coordinates.

At this point, matrix $A(x)$ is guaranteed to have minimal rank over all points in $\mathscr{S}$. This rank can be obtained as follows:

```
> SolveLMI(A,{rnk});
  [[x1 = [0, 0], x2 = [1, 1], rnk = 1]]
```

3.2 Degenerate spectrahedra

Let us modify the bottom right entry in the matrix of the previous section, so that now

$$A(x) = \begin{bmatrix} 1+x_1 & x_2 & 0 \\ x_2 & 1-x_1 & 0 \\ 0 & 0 & x_1-1 \end{bmatrix}$$

and the corresponding spectrahedron $\mathscr{S} = \{x \in \mathbb{R}^2 : A(x) \succeq 0\} = \{[1,0]\}$ reduces to a point in the plane. SPECTRA can easily deal with such a degenerate case:

```
> A := Matrix([[1+x1, x2, 0], [x2, 1-x1, 0], [0, 0, x1-1]]):
> SolveLMI(A);
  [[x1 = [1, 1], x2 = [0, 0]]]
```

Now let us modify further the bottom right entry, letting

$$A(x) = \begin{bmatrix} 1+x_1 & x_2 & 0 \\ x_2 & 1-x_1 & 0 \\ 0 & 0 & x_1-2 \end{bmatrix}$$

so that the corresponding spectrahedron is empty. SPECTRA returns the empty list, and this is a certificate of emptiness:

```
> A := Matrix([[1+x1, x2, 0], [x2, 1-x1, 0], [0, 0, x1-2]]):
> SolveLMI(A);
  []
```

Since SPECTRA is based on exact arithmetic, it is not sensitive to numerical roundoff errors or small parameter changes:

```
> A := Matrix([[1+x1, x2, 0], [x2, 1-x1, 0], [0, 0, x1-1-10^(-20)]]):
> SolveLMI(A);
  []
> A:=Matrix([[1+x1, x2, 0], [x2, 1-x1, 0], [0, 0, x1-1+10^(-20)]]):
> SolveLMI(A);
  [[x1 = [36893488147418995335 / 36893488147419103232,
          4611686018427401391 / 4611686018427387904],
    x2 = [-350142318592414077 / 247588007857076054979824844 8,
          -2801138548739304423 / 19807040628566084398385987584]]
```

Displayed with 10 significant digits, the latter point reads:

$$x_1 \in [\tfrac{36893488147418995 33}{36893488147419103232}, \tfrac{4611686018427401391}{4611686018427387904}] \approx 1.000000000,$$

$$x_2 \in [\tfrac{-350142318592414077}{2475880078570760549798248448}, \tfrac{-2801138548739304423}{19807040628566084398385987584}] \approx -0.1414213562 \cdot 10^{-9}.$$

The above point is an irrational solution, and the rational intervals are provided so that their floating point approximations are correct up to the number of digits specified in the Maple environment variable `Digits`, which is by default equal to 10. Use the command

```
> Digits:=100:
```

prior to calling `SolveLMI` if you want an approximation correct to 100 digits. At the price of increased computational burden, SPECTRA then provides larger integer numerators and denominators in the coordinate intervals.

3.3 Irrational spectrahedron

In general, each coordinate of a point computed by SPECTRA is an algebraic number, i.e. the root of a univariate polynomial with integer coefficients.

For the classical univariate matrix

$$A(x_1) = \begin{bmatrix} 1 & x_1 & 0 & 0 \\ x_1 & 2 & 0 & 0 \\ 0 & 0 & 2x_1 & 2 \\ 0 & 0 & 2 & x_1 \end{bmatrix}$$

the spectrahedron reduces to the irrational point $x_1 = \sqrt{2}$. The simple call

```
> A:=Matrix([[1, x1, 0, 0], [x1, 2, 0, 0], [0, 0, 2*x1, 2], [0, 0, 2, x1]]):
> SolveLMI(A);
  [[x1 = [26087635650665550353 / 18446744073709551616,
          13043817825332807945 / 9223372036854775808]]]
```

returns an interval enclosure valid to 10 digits. We can however obtain an exact representation of this point via a rational parametrization:

```
> SolveLMI(A, {par});
  [[x1 = [..], par = [_Z^2-2,_Z,[2]]]]
```

The output parameter `par` contains three univariate polynomials q, q_0, q_1 such that the computed point is contained in the finite set

$$\{q_1(z)/q_0(z) : q(z) = 0\} = \{2/z : z^2 - 2 = 0\} = \{\pm\sqrt{2}\}.$$

Here obviously the rational interval isolates the irrational point $x_1 = \sqrt{2}$.

3.4 Algebraic degree

The algebraic degree of semidefinite programming was studied in [5]. Let us consider the spectrahedron of Example 4 in this reference, for which

$$A(x) = \begin{bmatrix} 1+x_3 & x_1+x_2 & x_2 & x_2+x_3 \\ x_1+x_2 & 1-x_1 & x_2-x_3 & x_2 \\ x_2 & x_2-x_3 & 1+x_2 & x_1+x_3 \\ x_2+x_3 & x_2 & x_1+x_3 & 1-x_3 \end{bmatrix}.$$

The following point can be easily found with SPECTRA, and it has rank 2, which is guaranteed to be the minimal rank achieved in the spectrahedron:

```
> A:=Matrix([[1+x3, x1+x2, x2, x2+x3], [x1+x2, 1-x1, x2-x3, x2],
             [x2, x2-x3, 1+x2, x1+x3], [x2+x3, x2, x1+x3, 1-x3]]):
> SolveLMI(A, {rnk});
  [[x1 = [29909558235590963953/36893488147419103232,
          29909558235593946897/36893488147419103232],
    x2 = [-18555206088021567643/36893488147419103232,
          -9277603044010395249/18446744073709551616],
    x3 = [-12556837519724045701/36893488147419103232,
          -12556837519723709525/36893488147419103232],
    rnk = 2]]
```

With the following instruction we can indeed certify that there is no point of rank 1 or less:

```
> SolveLMI(A, {}, [1]);
  []
```

The command

```
> SolveLMI(A, {par});
```

returns the following rational univariate parametrization of the above rank 2 point:

$$
\begin{aligned}
q(z) &= 16144z^{10} + 35160z^9 + 14536z^8 - 17690z^7 - 16278z^6 - 2001z^5 + 1556z^4 + 454z^3 + 23z^2 - 4z - 1\\
q_0(z) &= 161440z^9 + 316440z^8 + 116288z^7 - 123830z^6 - 97668z^5 - 10005z^4 + 6224z^3 + 1362z^2 + 46z - 4\\
q_1(z) &= 97248z^9 + 146144z^8 - 18192z^7 - 134826z^6 - 63302z^5 + 4048z^4 + 6758z^3 + 846z^2 - 49z - 14\\
q_2(z) &= 34456z^9 + 37516z^8 - 8734z^7 - 22150z^6 - 8223z^5 - 3978z^4 - 1324z^3 + 104z^2 + 103z + 13\\
q_3(z) &= -35160z^9 - 29072z^8 + 53070z^7 + 65112z^6 + 10005z^5 - 9336z^4 - 3178z^3 - 184z^2 + 36z + 10
\end{aligned}
$$

so that the point belongs to the finite set

$$\left\{ \left(\frac{q_1(z)}{q_0(z)}, \frac{q_2(z)}{q_0(z)}, \frac{q_3(z)}{q_0(z)}, \frac{q_4(z)}{q_0(z)} \right) : q(z) = 0 \right\}.$$

The degree of the polynomial q in this parametrization can be obtained with the command

```
> SolveLMI(A, {deg});
```

We can obtain more points in the spectrahedron as follows:

```
> SolveLMI(A, {all, rnk, deg}, [2]);
```

This returns 4 feasible solutions of rank $r = 2$, all parametrized by the above degree 10 polynomial. Notice that this matches with the algebraic degree of a generic semidefinite programming problem with parameters $(m, n, r) = (4, 3, 2)$, which is 10 according to [5, Table 2].

3.5 Reproducibility

Consider the matrix

$$A(x) = \begin{bmatrix} 1+x_1 & x_2 \\ x_2 & 1-x_1 \end{bmatrix}$$

modeling the unit disk. Two consecutive calls to `SolveLMI` return two distinct points:

```
> A:=Matrix([[1+x1,x2],[x2,1-x1]]):
> SolveLMI(A);
 [[x1 = [-2120105604406202 7875/36893488147419103232, -662533001376936933/1152921504606846976],
   x2 = [-7548363607018988253/9223372036854775808, -1887090901754742967/2305843009213693952]]]
> SolveLMI(A);
   [[x1 = [-10862500438565607907/5902958103587056517 12, -2172500087713117721 5/11805916207174113034 24],
     x2 = [-576363141759828805/576460752303423488, -9221810268157244495/9223372036854775808]]]
```

After another call, or on your own computer, these intervals should still differ as SPECTRA makes random changes of coordinates to ensure that the geometric objects computed are in general position. This kind of behavior is expected when there are infinitely many points of minimal rank in the spectrahedron.

To generate reproducible outputs, the instruction `randomize` can be used to seed the random number generator used by Maple:

```
> randomize(31415926):
> SolveLMI(A);
  [[x1 = [-35204733513421104993/36893488147419103232, -35204733513421000447/36893488147419103232],
    x2 = [-2758579864857623899/9223372036854775808, -5517159729715231413/18446744073709551616]]]
> randomize(31415926):
> SolveLMI(A);
  [[x1 = [-35204733513421104993/36893488147419103232, -35204733513421000447/36893488147419103232],
    x2 = [-2758579864857623899/9223372036854775808, -5517159729715231413/18446744073709551616]]]
```

3.6 Polynomial sums of squares

Deciding whether a multivariate real polynomial is non-negative is difficult in general. A sufficient condition, or certificate for non-negativity, is that the polynomial can be expressed as a sum of squares (SOS) of other polynomials. Finding a polynomial SOS decomposition amounts to finding a point in a specific spectrahedron called Gram spectrahedron, see e.g. [1] and references therein.

As an example, consider the homogeneous ternary quartic

$$f(u) = u_1^4 + u_1u_2^3 + u_2^4 - 3u_1^2u_2u_3 - 4u_1u_2^2u_3 + 2u_1^2u_3^2 + u_1u_3^3 + u_2u_3^3 + u_3^4.$$

The polynomial f belongs to a series of examples produced by C. Scheiderer in [6] to answer (in the negative) the following question by B. Sturmfels: let f be a polynomial with rational coefficients which is an SOS of polynomials with real coefficients; is it an SOS of polynomials with rational coefficients? Scheiderer's counterexamples prove that, generally speaking, there is no hope in obtaining nonnegativity certificates over the rationals. However, certificates exist in some algebraic extension of the field of rational numbers.

In the graded reverse lexicographic ordered monomial basis, the Gram matrix of f is the matrix

$$A(x) = \begin{bmatrix} 1 & 0 & x_1 & 0 & -3/2 - x_2 & x_3 \\ 0 & -2x_1 & 1/2 & x_2 & -2 - x_4 & -x_5 \\ x_1 & 1/2 & 1 & x_4 & 0 & x_6 \\ 0 & x_2 & x_4 & -2x_3 + 2 & x_5 & 1/2 \\ -3/2 - x_2 & -2 - x_4 & 0 & x_5 & -2x_6 & 1/2 \\ x_3 & -x_5 & x_6 & 1/2 & 1/2 & 1 \end{bmatrix}$$

depending linearly on 6 real parameters. The Gram spectrahedron $\mathscr{S} = \{x \in \mathbb{R}^6 : A(x) \succeq 0\}$ parametrizes the set of all SOS decompositions of f. We deduce by the discussion above that $\mathscr{S}$ does not contain rational points. In particular, its interior is empty.

Let us use SPECTRA to compute points in $\mathscr{S}$ and hence to get positivity certificates for f:

```
> A := Matrix([[1,0,x1,0,-3/2-x2,x3], [0,-2*x1,1/2,x2,-2-x4,-x5], [x1,1/2,1,x4,0,x6],
               [0,x2,x4,-2*x3+2,x5,1/2], [-3/2-x2,-2-x4,0,x5,-2*x6,1/2], [x3,-x5,x6,1/2,1/2,1]]):
> out := SolveLMI(A, {rnk, deg, par});
          -8581452335803113365  -4290726167901519779          -4611686018427402223  -9223372036854747171
 [[[x1 = [--------------------, --------------------], x2 = [--------------------, --------------------],
          9223372036854775808   4611686018427387904           4611686018427387904   9223372036854775808

          6745044697806705179  1686261174451679625          -4956654678096131785  -4956654678096116467
    x3 = [--------------------, --------------------], x4 = [--------------------, --------------------],
          9223372036854775808  2305843009213693952           1844674407370955161 6  1844674407370955161 6

          4290726167901543733  536340770987693255          -8581452335803091439  -2145363083950772283
    x5 = [--------------------, ------------------], x6 = [--------------------, --------------------]],
          4611686018427387904  576460752303423488          9223372036854775808   2305843009213693952

    rnk = 2, deg = 3,
    par = [8*z^3+8*z+1, 24*z^2-8, [16*z+3, -24*z^2+8, 8*z^2+6*z+8, -16*z^2+6*z+16, -16*z-3, 16*z+3]]]
```

We obtain an irrational point $x \in \mathscr{S}$ whose coordinates are algebraic numbers of degree 3, and which belongs to the finite set

$$\left\{ \left(\frac{16z+3}{24z^2-8}, \frac{-24z^2+8}{24z^2-8}, \frac{8z^2+6z+8}{24z^2-8}, \frac{-16z^2+6z+16}{24z^2-8}, \frac{-16z-3}{24z^2-8}, \frac{16z+3}{24z^2-8} \right) : 8z^3 - 8z - 1 = 0 \right\}$$

At this point, the Gram matrix A has rank 2, and hence f is an SOS of 2 polynomials.

Let us compute more non-negativity certificates of rank 2:

```
> out:=SolveLMI(A,{rnk,deg,par,all},[2]);
```

In addition to the point already obtained above, we get another point. The user can compare this output with [6, Ex. 2.8]: it turns out that these are the only 2 points of rank 2. Other points in the Gram spectrahedron have rank 4 and they are convex combinations of these 2.

4 Input

The calling sequence of function `SolveLMI` is as follows:

```
> SolveLMI(A, options, ranks);
```

where

- A is a symmetric matrix of size m with rational coefficients, depending affinely on n variables;
- `options` (optional) is a set that can contain the following keywords:

  `all` : compute as many solutions as possible, which can be computationally demanding; when this option is not specified, the algorithm is stopped as soon as one solution is computed, which is typically much faster;

  `rnk` : return the rank of A at every computed solution;

  `par` : return the rational univariate parametrization of every computed solution;

  `deg` : return the algebraic degree of every computed solution;
- `ranks` (optional) is a list of nonnegative integers corresponding to expected ranks of computed solutions. The default value is $[0, 1, \ldots, m-1]$. The algorithm is run for each value r in `ranks` by solving the quadratic system of equations

  $$A(x)Y(y) = 0$$

  for a vector x and a matrix $Y(y)$ with m rows and $m - r$ columns whose entries are stored in a vector y. It may happen that the rank of $A(x)$ at a computed solution x is strictly less than r.

5 Output

Let us denote by $x_1, x_2, \ldots, x_n$ the variables on which matrix A depends affinely. They are gathered in a vector $x \in \mathbb{R}^n$. When the input argument `options` is empty, the output returned by `SolveLMI` is

- eithter the empty list `[]` in which case $\mathscr{S}$ is empty, or
- a rational enclosure of a single point $x \in \mathscr{S}$, in the form

  ```
  > SolveLMI(A)
    [[x1 = [a1, b1], x2 = [a2, b2], ..., xn = [an, bn]]]
  ```

  where a_i, b_i are rational numbers, displayed as ratios of integers. This means that each coordinate x_i belongs to the interval $[a_i, b_i]$ ensuring a floating point approximation of x valid to a number of digits equal to the Maple environment variable `Digits`. When $a_i = b_i$ this implies that x_i is a rational number.

When `options` contains the keyword `all`, more points can be returned, in the form of a list

```
> out := SolveLMI(A, {all})
  [[x1 = [a11, b11], x2 = [a12, b12], ..., xn = [a1n, b1n]],
   [x1 = [a21, b21], x2 = [a22, b22], ..., xn = [a2n, b2n]],
   ...]
```

such that `nops(out)` is the number of computed points, `out[1]` is the first point, `out[2]` is the second point, etc.

When `options` contains the keyword `rnk`, the rank of A at x is returned:

```
> SolveLMI(A, {rnk})
  [[x1 = [a1, b1], x2 = [a2, b2], ..., xn = [an, bn], rnk = r]]
```

These keywords and the following ones can be freely combined:

```
> SolveLMI(A, {all, rnk})
  [[x1 = [a11, b11], x2 = [a12, b12], ..., xn = [a1n, b1n], rnk = r1],
   [x1 = [a21, b21], x2 = [a22, b22], ..., xn = [a2n, b2n], rnk = r2],
   ...]
```

When `options` contains the keyword `par`, a rational univariate parametrization of x is returned:

```
> SolveLMI(A, {par})
  [[x1=[a1,b1], x2=[a2,b2], ..., xn=[an,bn], par=[q,q0,[q1,q2,...,qn]]]
```

This parametrization is such that $q, q_0, q_1, q_2, \ldots, q_n$ are univariate polynomials with integer coefficients such that x belongs to the finite set

$$\left\{ \left(\frac{q_1(z)}{q_0(z)}, \frac{q_2(z)}{q_0(z)}, \cdots, \frac{q_n(z)}{q_0(z)} \right) : q(z) = 0,\ z \in \mathbb{C} \right\}.$$

The intervals $[a_i, b_i]$ are provide to isolate the computed point from this set of points.

When `options` contains the keyword `deg`, the degree of the polynomial q in the rational univariate parametrization of each computed point x is also returned:

```
> SolveLMI(A, {deg})
  [[x1 = [a1, b1], x2 = [a2, b2], ..., xn = [an, bn], deg = d]]
```

References

[1] L. Chua, D. Plaumann, R. Sinn, C. Vinzant. Gram spectrahedra. `arXiv:1608.00234`, July 2016.

[2] J.-C. Faugère. FGb: a library for computing Gröbner bases. In K. Fukuda, J. van der Hoeven, M. Joswig, N. Takayama, editors, Mathematical Software - ICMS 2010, volume 6327 of Lecture Notes in Computer Science, pp. 84-87, Springer, Berlin, 2010. Software available at `www-polsys.lip6.fr/~jcf/FGb`

[3] D. Henrion, S. Naldi, M. Safey El Din. Exact algorithms for linear matrix inequalities. `arXiv:1508.03715`, Aug. 2015. To appear in SIAM J. Opt.

[4] S. Naldi. Exact algorithms for determinantal varieties and semidefinite programming. PhD thesis, Univ. Toulouse and Univ. Pierre et Marie Curie Paris. `tel.archives-ouvertes.fr/tel-01212502`, Oct. 2015.

[5] J. Nie, K. Ranestad, B. Sturmfels. The algebraic degree of semidefinite programming. Math. Prog. 122(2):379-405, 2010.

[6] C. Scheiderer. Sums of squares of polynomials with rational coefficients. J. Eur. Math. Soc. 18(7):14951513, 2016.